KASPERSKY lab

KASPERSKY SECURITY FOR BUSINESS PORTFÖYÜ 2015

"KURULUŞUNUZU KORUYAN GÜÇ"

Tüm işletmeler büyüklüklerinden bağımsız olarak kötü amaçlı yazılım saldırısı tehdidi altındadır. Kaspersky Lab, bu tehditlerin büyük bir bölümünü algılama ve keşfetme alanında benzersiz bir deneyime sahiptir.

Tehdit seviyesi yükselmeye devam ediyor. Her gün bireyleri ve sizinki gibi işlemeleri hedef alan 325.000'in üzerinde benzersiz tehdit üretilmektedir.

Kaspersky Lab'da bizler bu tehditler ve işletmeniz için ortaya çıkardığı riskle ilgileniriz. Bu deneyim ışığında, sizinki gibi bize danışmanlık için başvuran kuruluşlara BT güvenlik stratejilerinin üç önemli kriteri karşıladığından emin olmalarını öneririz:

- **İlk olarak,** üstün bir tehdit istihbaratına erişim sağlamalısınız. Bu istihbarat tehdidin görünümü, yazılma ve derlenme yöntemleri hakkında derin bir anlayış sağlar. Güvenlik sisteminizin uzman bilgileri tarafından sürekli olarak beslenmesi ve tedarikçinizin yaklaşan tehditleri görebilmek için kötü amaçlı yazılımın yoğun olduğu bölgeleri gözlem altında tutması gerekir.

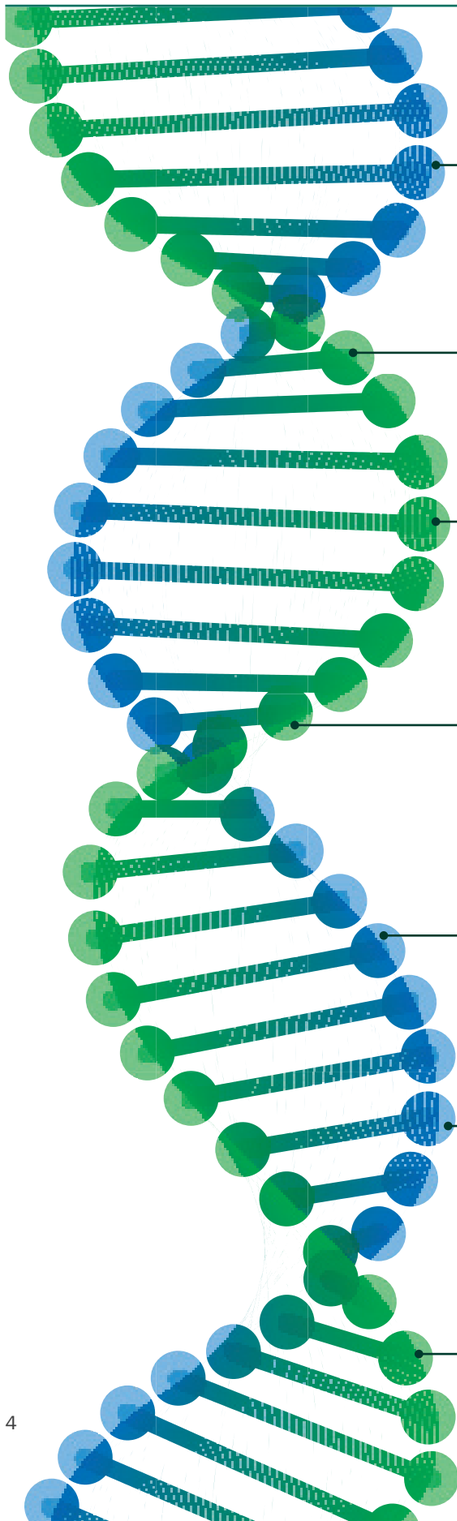
- **İkinci olarak,** güvenliğiniz bilinen, bilinmeyen ve gelişmiş kötü amaçlı yazılımları algılama ve ortadan kaldırma becerisine sahip olmalıdır. Güvenlik yazılımınız aynı zamanda sistemleriniz üzerindeki yükü azaltarak ve hızlı tarama süreleri sağlayarak işletmenizi sekteye uğratmamalıdır.

- **Üçüncü kriter,** her gün daha karmaşık hale gelen işletme BT ortamlarına yöneliktir. Bu yeni durum, teknolojinin fiziksel, mobil ve sanal uç noktalara yazılım çatışmaları, birden fazla konsol veya güvenlik boşluğu olmadan, tek bir platformla sorunsuz ve verimli şekilde erişmesini gerekli kılmaktadır.

İşletmenizin ihtiyaç duyduğu dünya lideri tehdit istihbaratı sadece Kaspersky tarafından sunulur ve bu sistemin çalışmasına olanak sağlayan teknoloji kapsamlı bir güvenlik platformunda yerleşik olarak bulunur.

Kaspersky çözümleri, işletme hedeflerinizle uyumlu hale gelebilmelerini sağlayan esneklikle tasarlanır. Bu yaklaşım, fiziksel ve sanal uç noktalarınızı, mobil cihazlarınızı hedefleyen tehditlere karşı kuruluşunuzu savunmak için her zaman hazır olmamızı sağlar. Posta sistemleriniz, sunucularınız, ağ geçitleriniz ve SharePoint portallarınız. Bu belgede açıklanan tüm ürünler, çözümler ve hizmetler için BT bayinizle bugün iletişim kurun. Size işletmenizi siber tehditlere korumak amacıyla nasıl birlikte çalışabileceğimizi göstermemize izin verin.

GÜVENLİK İSTİHBARATI DNA'MIZA İŞLEMİŞTİR



Tepeden tırnağa uzmanlık

GREAT ekibiyle küresel tehdit istihbaratında lider

En iyi güvenlik kuruluşlarının saygısını kazanmış

Teknoloji odaklı

Bağımsız testlerde liderliği ispatlanmış

En karmaşık tehditlerin algılanmasında lider

Kaspersky Security Network ile güvenlik olaylarını görün ve önlem alın

FARK YARATAN GÜVENLİK

Kaspersky Lab, DNA'mıza işleyen, tüm faaliyetlerimizi ve yöntemlerimizi etkileyen dünya lideri güvenlik istihbaratı oluşturarak piyasadaki en güçlü kötü amaçlı yazılımlara karşı koruma platformunu sunar.

- CEO'muz Eugene Kaspersky'den başlayacak şekilde tepeden tırnağa teknolojiye inanan bir şirketiz.
- Küresel Araştırma ve Analiz Ekibimiz (GReAT), dünyanın en tehlikeli kötü amaçlı yazılım tehditlerini ve hedefe yönelik saldırıları herkesten önce ortaya çıkaran elit BT güvenlik uzmanlarından oluşan bir gruptur.
- Dünyanın birçok saygıdeğer güvenlik kuruluşu ve emniyet güçleri aktif olarak yardımımıza başvurmaktadır.
- Kaspersky Lab'ın tüm temel teknolojilerini şirket bünyesinde geliştirmesi ve mükemmel hale getirmesi, ürünlerimizin doğal olarak daha dengeli ve daha etkili olmasını sağlar.
- Kaspersky Lab her yıl tüm diğer tedarikçilere göre çok daha fazla bağımsız teste katılır ve bu testlerden rakip tedarikçilere göre çok daha başarılı sonuçlar alır!
- En güvenilir sektör analizi şirketleri (Gartner, Inc, Forrester Research ve International Data Corporation (IDC) dahil olmak üzere) birçok önemli BT güvenlik kategorisinde bizi Lider olarak kabul etmektedir
- 130'un üzerinde OEM (Microsoft®, Cisco® Meraki, Juniper Networks, Alcatel Lucent ve daha fazlası) kendi ürünleri ve hizmetlerinde bizim teknolojilerimizi kullanmaktadır.

Farkı yaratan da budur!

▶ KÖTÜ AMAÇLI YAZILIMDAN KORUMA TEKNOLOJİMİZ HAKKINDA

BT güvenlik yazılımı, merkezindeki güvenlik motoru kadar etkindir. Yama yönetimi, MDM, şifreleme, cihaz kontrolleri, kimlik avı koruması gibi birçok teknoloji ve fazlası, değerli ek güvenlik katmanları sağlar. Kuruluşlar bilinen, bilinmeyen ve gelişmiş tehditlere karşı güvenlikten ödün verme şansına sahip değildir.

Kaspersky Lab'ın güvenlik motoru, benzersiz ve dinamik tehdit istihbaratımızın desteğiyle sürekli olarak güçlenmekte ve entegre hale gelmektedir. Tek odak noktası olarak güvenliği belirlememiz, tehdit istihbaratımız ve küresel deneyimimizle birleştiğinde diğerlerinden ayrılmamızı sağlar.

Kaspersky Endpoint Security for Business platformunda yerleşik olarak bulunan kötü amaçlı yazılımdan koruma motorunun sektör lideri performansı, çok sayıda ve kesintisiz bağımsız testlerle ispatlanmıştır. Kaspersky güvenliğinin benzersizliği sizin tespitlerinizle de onaylanmıştır.

Kaspersky Lab tarafından üretilen kötü amaçlı yazılım korumasını diğerlerinden çok daha güçlü ve etkili hale getiren birkaç özelliği burada görebilirsiniz.

TEMEL ÜRÜN ÖZELLİKLERİ

- **Bilinen, Bilinmeyen ve Gelişmiş Tehditleri Algılama**
- **Davranış Analizi ve Sezgisel Araçlar**
- **Bulut Destekli Koruma için Kaspersky Security Network**
- **Etkin Temizleme**
- **Şifreleme ve Ransomware Savunması**
- **Otomatik Güvenlik Açıklarını Önleme**
- **HIPS ve Kişisel Güvenlik Duvarı**
- **Ağ Saldırısı Engelleyici**
- **Basit, Şeffaf Yönetim Konsolu**

ÖNE ÇIKAN NOKTALAR

ÇOK KATMANLI YAKLAŞIM

Kaspersky Lab'ın çok katmanlı yaklaşımı bugün piyasadaki en etkili güvenliği sağlayabilmemizin nedenlerinden biridir. Kaspersky Lab teknolojilerinin şirket içinde geliştirilmesi, güçlü ve düzenli koruma katmanlarının performansa en az etkide bulunarak birlikte sorunsuz şekilde çalışabilmelerini sağlar.

Her bir koruma katmanı siber tehditleri farklı bir bakış açısıyla ele alarak BT profesyonellerinin birbiriyle kenetlenen teknolojiler uygulamalarına, derin ve kapsamlı güvenlik sağlamalarına imkan tanır.

DÜNYA LİDERİ TEHDİT İSTİHBARATI KESİNTİSİZ KORUMANIN GARANTİSİDİR

Kaspersky Lab'ın Küresel tehdit istihbaratı dünya çapında tanınmaktadır ve bu uzmanlık doğrudan sürekli gelişen BT dünyasına uyum sağlayan güvenlik çözümlerimize yansıtılır.

ÖZELLİKLER

SİSTEMLERİNİZDEKİ YÜKÜ AZALTAN SEZGİSEL GÜVENLİK

Şablon tabanlı kötü amaçlı yazılım tanılaması, algılama oranını yükseltmenin yanı sıra daha küçük güncelleme dosyaları ve daha fazla güvenlik sağlar.

DAVRANIŞ ANALİZİ

Kaspersky kötü amaçlı yazılımdan koruma çözümünde program etkinlik analizi için iki özel bileşen bulunur:

- Programın hedeflenen etkinliklerini çalıştıran ve doğrulayan **emülatör**.
- Çalışmakta olan programların etkinliklerini izleyen, kötü amaçlı yazılımların davranış şablonu özelliklerini sezen ve analiz eden **Sistem İzleyici**.

BULUT DESTEKLİ KÖTÜ AMAÇLI YAZILIM KORUMASI – KASPERSKY SECURITY NETWORK (KSN)

Yeni ve bilinmeyen kötü amaçlı yazılım tehditlerine gerçek zamanlı yanıt. Kötü amaçlı yazılım saldırıları ve şüpheli davranışlara yönelik 60 milyonun üzerinde Kaspersky Lab yazılım kullanıcısı tarafından gönüllü olarak sağlanan yeni ve anlık veri akışı, tehditlerin hızlı şekilde yanıtlanması için kullanılır. Bu yaklaşım, müşterilerin gerçek zamanlı korumadan daha az "yanlış tespitle" faydalanmasına olanak sağlar.

OTOMATİK GÜVENLİK AÇIKLARINI ÖNLEME

Popüler uygulamaların güvenlik açıklarını ortaya çıkaran kötü amaçlı yazılımları hedef alan Otomatik Güvenlik Açıklarını Önleme özelliği, tipik veya şüpheli davranış şablonlarını algılar. Teknoloji daha sonra güvenlik açıklarını izleyerek ortadan kaldırır ve indirilen kötü amaçlı kodların çalıştırılmasını önler.

ŞİFRELEME RANSOMWARE (FİDYE YAZILIMI) KARŞI ÖNLEMLERİ

Sistem İzleyici, şüpheli bir işlemin önemli dosyalara erişmeyi denemesi ihtimaline karşın önemli dosyaların kopyalarını geçici depolama alanında saklar. Fidye yazılımının orijinalleri şifrelemeyi denemesi durumunda, bu dosyalar şifrelenmemiş durumuna geri yüklenir.

ETKİN TEMİZLEME

Algılanan tüm virüs bulaşmalarının "iyileştirilmesinde" dosya ve işlemin çalıştırılmasını önleyen otomatik başlatma, kötü amaçlı yazılımı yok etme ve depolanan belgeleri orijinal durumuna döndüren "geri sarma" gibi teknikler kullanılır.

ANA BİLGİSAYAR TABANLI İZİNSİZ GİRİŞ ÖNLEME SİSTEMİ (HIPS) VE KİŞİSEL GÜVENLİK DUVARI

Bazı program etkinlikleri, kötü amaçlı oldukları onaylanmasa bile kısıtlama önerilmesine yetecek kadar büyük risk taşır. Ağ etkinliğini kısıtlayan uygulama düzeyinde Kişisel Güvenlik Duvarı'ndan yardım alan Kaspersky Lab'ın Ana Bilgisayar Tabanlı İzinsiz Giriş Önleme Sistemi (HIPS), uygulamanın güvenlik düzeyine bağlı olarak sistem içindeki etkinliklerini kısıtlar.

AĞ SALDIRISI ENGELLEYİCİ

Ağınızdaki şüpheli faaliyetleri izler ve şüpheli bir davranışın algılanması durumunda sisteminizin nasıl yanıt vereceğini önceden tanımlamanızı sağlar.

SIK GÜNCELLEMELER

Yeni kötü amaçlı yazılımlara karşı koruma sağlayan güncellemeler, Kaspersky Security Network (KSN) bulut platformundan gelen ve yeni keşfedilen kötü amaçlı yazılımlar hakkında sürekli güncellenen verilerle birlikte güvenlik veritabanınıza sektördeki en hızlı güncelleme döngüsüyle iletilir.

SEKTÖR LİDERİ KORUMA — BAĞIMSIZ OLARAK ONAYLANAN GERÇEK

Kaspersky Lab ürünleri 2014 yılı boyunca **93 bağımsız test ve incelemeye katılmıştır.** Ürünlerimiz bu testlerin **66 tanesini ilk üç içerisinde bitirerek**, **%71 İLK 3 oranına** sahip olmuş ve katıldığı testlerin yarısından fazlasında, **51 testte** ilk sırayı almıştır.

Önde gelen rakiplerimizin hiçbir ürünü veya çözümü bu sonuçlara yaklaşamamıştır.

İŞLETMELER İÇİN GÜVENLİK ÜRÜNLERİ, ÇÖZÜMLERİ VE HİZMETLERİ

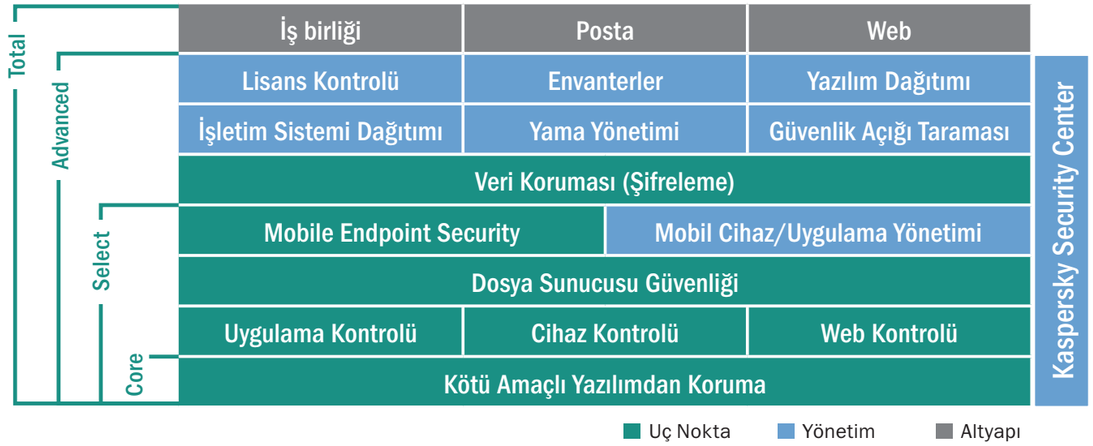
Kaspersky Endpoint Security for Business	Dünyanın en gelişmiş tehdit istihbaratı ekosisteminden faydalanan Kaspersky Endpoint Security for Business, tek ve entegre bir platform üzerine kurulu katmanlı bir güvenlik yaklaşımı sunar. Bu platform, güvenilir uygulama, cihaz ve web kontrol araçları, veri şifreleme, mobil uç nokta güvenliği ve MDM'nin yanı sıra sistem ve yama yönetimi gibi özellikler sağlar. Her şey tek bir merkezi konsol olan Kaspersky Security Center'dan yönetilir. Kaspersky Total Security for Business posta, web ve işbirliği sunucusu güvenliği, bölgenizin ve tüm kurumsal BT ortamınızın güvenliğini sağlar.
Kaspersky Hedeflenen Çözümler	Kaspersky Lab güvenliğinin BT sisteminizin belirli bölgelerine uygulanmasına olanak sağlayan bağımsız çözümler. Kaspersky Security for Mobile gibi bazı çözümler, Kaspersky Endpoint Security for Business'ın bir parçası olarak bulunur. Kaspersky Security for Virtualization gibi diğerleri ise tamamen hedefe yönelik çözümler olarak bulunur. En gelişmiş teknolojiler ve tehdit istihbaratının üzerine inşa edilen bu çözümlerin yanı sıra tüm fiziksel, mobil ve sanal uç nokta çözümleri Kaspersky Security Center ile merkezi olarak kontrol edilirler.
Kaspersky Güvenlik İstihbaratı Hizmetleri ve Kurumsal Çözümler	Kaspersky'nin tehdit istihbaratı, teknik uzmanlığı, veri ve eğitim becerilerinden faydalanarak markanızın, kuruluşunuzun ve çalışanlarınızın güvenliğine katkıda bulunurlar Kurumsal Çözümler, belirli sektörler ve altyapılara yönelik güvenlik sorunlarını ve Dağıtılmış Hizmet Reddi (DDoS) gibi özel araç biçimlerini etkisiz hale getirir.
KASPERSKY SMALL OFFICE SECURITY	Birinci sınıf koruma, küçük işletmelere uyumlu hale getirildi.
BAKIM VE HİZMET SÖZLEŞMELERİ	Kaspersky güvenlik çözümünüze yönelik geniş bir destek seçenekleri yelpazesi.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS HAKKINDA

Kaspersky Endpoint Security for Business dünyanın önde gelen güvenlik uzmanları tarafından tasarlanmış eksiksiz bir güvenlik çözümü sağlar. İşinizi tamamen koruma altına almak için en derin, en ileriye dönük koruma, etkili performans ve sürekli gelişen katmanlar ile kurulmuş basit yönetim.

Tüm bileşenler işinizin ihtiyaçlarına göre ayarlanmış tek bir platformda bir araya gelmeleri için şirket bünyesinde tasarlanmış ve oluşturulmuştur. Bunun sonucunda boşluksuz, uyum sorunu olmayan ve güvenlik gereksiniminiz büyüdükçe ekstra iş gücü yükü çıkarmayan dengeli ve entegre bir çözüm ortaya çıkar.

Yöneticiler Kaspersky Endpoint Security for Business ile BT ortamlarını görebilir, kontrol edebilir ve koruyabilir. Araçlar ve teknolojiler gelişen güvenlik ve BT ihtiyaçlarınızı karşılamak için gelişen katmanlar boyunca eşsiz bir şekilde dengelenir. Kaspersky işinizi kolaylaştırabilir.

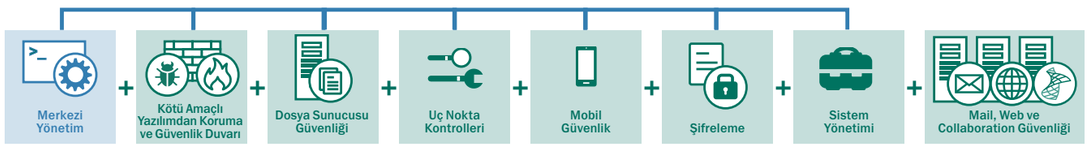


Kaspersky kapsamlı bir teknoloji listesine sahip olmaktan gurur duyar. Bu teknolojilerin tümü müşterilerimize ihtiyaç duydukları birinci sınıf korumayı sağlayabilmek için aynı kod tabanı ile birlikte çalışır ve bulut tabanlı Kaspersky Security Network ile de desteklenir.

Kısacası sektörün ilk Güvenlik Platformunu sıfırdan oluşturarak sunduk ve bu da yöneticilerin kendi dünyalarını görmelerini, kontrol etmelerini ve korumalarını kolaylaştırdı.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Sektörün önde gelen güvenlik uzmanları tarafından tasarlanan ve geliştirilen, bilinen, bilinmeyen ve gelişmiş çözümlere karşı çok katmanlı güçlü koruma. Dünya çapında tanınan tehdit istihbaratı tarafından desteklenen Kaspersky Endpoint Security for Business, benzersiz BT güvenliği ve kontrol sağlar.



KASPERSKY ENDPOINT SECURITY FOR BUSINESS — CORE

Kaspersky Lab güvenlik platformunun temelini oluşturan, sınıfının en iyisi kötü amaçlı yazılımdan koruma

Kaspersky Lab'ın çok katmanlı koruma teknolojileri, güvenlik konusunda tutkulu kişiler tarafından şirket bünyesinde geliştirilmiştir. Bağımsız testler tarafından da onaylanan sonuç, kuruluşunuz için en iyi korumayı sağlayan, sektörün en güçlü ve etkili güvenlik çözümüdür.

Bilinen, Bilinmeyen ve Gelişmiş Tehditlere Karşı Koruma — benzersiz, gelişmiş teknolojiler, mevcut ve büyümekte olan tehditleri algılar ve ortadan kaldırır.

Otomatik Güvenlik Açıklarını Önleme — proaktif şekilde bilinmeyen ve gelişmiş tehditleri hedef alır.

Bulut Destekli Koruma — Dünya çapındaki Kaspersky Security Network'ten gelen gerçek zamanlı bilgileri kullanır.

Sistem İzleyici — Sistemin etkilenmesi durumunda benzersiz dosya geri yükleme işlevi sunar.

Ana Bilgisayar Tabanlı İzinsiz Giriş Önleme Sistemi (HIPS) ve Kişisel Güvenlik Duvarı — Ağ etkinliğini kısıtlayan uygulama düzeyinde Kişisel Güvenlik Duvarı destekli HIPS, etkinlikleri uygulamanın güvenilirlik düzeyine bağlı olarak kısıtlar.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS — SELECT

Mobil cihaz ve veri güvenliği için güçlü, parçalı uç nokta kontrolleri, proaktif güvenlik ve yönetimle birleştirilir

Kaspersky'nin benzersiz dinamik beyaz liste desteği dahil olmak üzere uygulama, web ve cihaz kontrolleri, derin uç nokta güvenliği anlayışına yeni bir boyut kazandırır. Kurumlara ve çalışanlara ait (BYOD) mobil cihazlar korunur ve korunan tüm uç noktaların dahil olduğu platformlar Kaspersky Security Center konsolundan yönetilecek şekilde birleştirilir. Dosya sunucusu koruması virüsün depolanmış veriler aracılığıyla güvenli uç noktaya yayılamayacağını garanti eder.

UÇ NOKTA KONTROLLERİ

Dinamik Beyaz Liste ile Uygulama Kontrolü— Kaspersky Security Network tarafından sağlanan gerçek zamanlı dosya itibar değerlerini kullanarak, BT yöneticilerinin uygulamalara izin vermesine, engellemesine veya düzenlemesine olanak sağlar. Bu çözüm ayrıca "Varsayılan Olarak Reddet" beyaz liste senaryosunun canlı olarak veya test ortamında uygulanmasına imkan tanır. Uygulama Ayrıcalık Kontrolü ve Güvenlik Açığı Taraması, uygulamaları izler ve şüpheli davranan uygulamaları kısıtlar.

Web Kontrolü — gezinme ilkelerinin önceden belirlenen veya özelleştirilebilen kategoriler etrafında oluşturulabilmesi, kapsamlı gözetim ve yönetim etkinliği sağlar.

Cihaz Kontrolü — çıkarılabilir depolama cihazları ve diğer çevre birim cihazlarının bağlantı durumunu kontrol eden parçalı veri ilkeleri, birden fazla cihazın eşzamanlı dağıtımına yönelik maskeler kullanılarak ayarlanabilir, planlanabilir ve uygulanabilir.

DOSYA SUNUCUSU GÜVENLİĞİ

Kaspersky Security Center ile uç nokta güvenliğiyle birlikte yönetilir.

MOBİL GÜVENLİK:

Mobil Cihazlar için Güçlü Güvenlik — çok katmanlı gerçek zamanlı mobil uç nokta koruması sağlamak için gelişmiş, proaktif ve bulut destekli teknolojiler bir arada kullanılır.

Web koruması, anti-spam ve kimlik avı koruması bileşenleri cihaz güvenliğine katkıda bulunur.

Uzaktan Hırsızlığa Karşı Koruma — Kilitleme, Silme, Konum Belirleme, SIM İzleme, Alarm, Gizli Fotoğraf Çekme ve Tam veya Seçmeli Silme özelliklerinin tümü, mobil cihazın kaybolması veya çalınması durumunda kurumsal verilere izinsiz erişimi önler. Yönetici ve son kullanıcı tarafından etkinleştirmenin yanı sıra Google Cloud Management desteği, gerektiğinde hızlı aktivasyon sağlar.

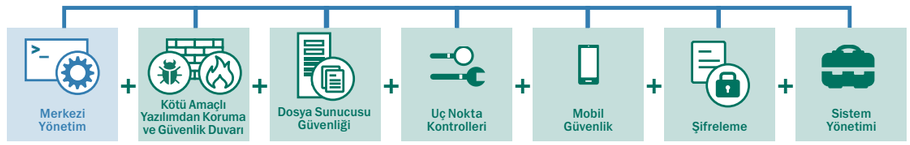
Mobil Uygulama Yönetimi (MAM) — Kullanıcının sadece beyaz listede yer alan uygulamaları çalıştırmasını sağlayarak, istenmeyen veya bilinmeyen yazılımların dağıtılmasını önler. "**Uygulama Paketleme**" çalışanlara ait cihazlarda kurumsal verileri kişisel verilerden ayırır. Ek şifreleme veya "Seçmeli Silme" özellikleri uzaktan uygulanabilir.

Mobil Cihaz Yönetimi (MDM) — **Microsoft® Exchange ActiveSync** ve **iOS MDM** cihazlar için OTA (Kablosuz) ilke dağıtımı sağlayan birleşik arabirim. Android™ tabanlı cihazlar için **Samsung KNOX** desteklenir.

Self Servis Portal — çalışana ait onaylı cihazların ağa otomatik kaydedilmesini sağlar. Bu işlem sırasında tüm gerekli sertifikalar ve anahtarlar otomatik olarak yüklenir. Hırsızlığa karşı koruma özelliklerinin acil durumlarda kullanıcı/cihaz sahibi tarafından etkinleştirilebilmesi BT yönetim iş yükünü azaltır.

Kaspersky Endpoint Security for Business — SELECT çözümü CORE katmanının tüm bileşenlerini içerir.

▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS — ADVANCED



Sistem yönetim araçları BT verimliliği ve güvenliğini optimize ederken, entegre şifreleme hassas verileri korur

Otomatik yama yönetimi ve İşletim Sistemi görüntüsü yönetimi, uzaktan yazılım dağıtımı ve SIEM entegrasyonu özelliklerinin tümü yönetimin sadeleştirilmesine katkıda bulunurken, donanım ve yazılım envanterleri ve lisans yönetimi görünürlük ve kontrol sağlar. Entegre şifreleme teknolojisi çözüme güçlü bir veri koruma katmanı ekler.

SİSTEM YÖNETİMİ

Güvenlik Açığı ve Yama Yönetimi **— yamaların ve güncellemelerin hızlı ve otomatik dağıtımı ile birleştirilmiş otomatik işletim sistemi ve uygulama güvenlik açığı algılama ve öncelik belirleme.**

İşletim Sistemi Dağıtımı— İşletim Sistemi "sanal kopya" görüntülerini UEFI desteği sunan merkezi bir konumdan kolayca üretme, depolama ve dağıtma.

Yazılım Dağıtımı ve Sorun Giderme — uzaktan yazılım dağıtımının yanı sıra uygulama ve İşletim Sistemi güncellemeleri, LAN Uyanması desteğiyle talebe göre veya planlı olarak gerçekleştirilir. Zaman tasarrufu sağlayan uzaktan sorun giderme ve verimli yazılım dağıtımı Multicast teknolojisiyle desteklenir.

Donanım ve Yazılım Envanterleri ve Lisans Yönetimi— tanımlama, görünürlük ve kontrolle (engelleme dahil) birlikte sunulan lisans kullanımı yönetimi, ortamda dağıtılan tüm yazılım ve çıkarılabilen cihazları içerecek şekilde donanımlara yönelik bilgi sağlar. Yazılım ve donanım lisans yönetimi, konuk cihaz algılama, öncelik kontrolleri ve erişim sağlama özellikleri kullanılabilir.

SIEM Entegrasyonu — IBM® QRadar ve HP ArcSight SIEM sistemlerine yönelik destek.

Rol Tabanlı Erişim Kontrolü (RBAC) — Karmaşık ağlardaki yönetim sorumlulukları, atanan roller ve haklara göre özelleştirilen konsol görünümleriyle atanabilir

ŞİFRELEME

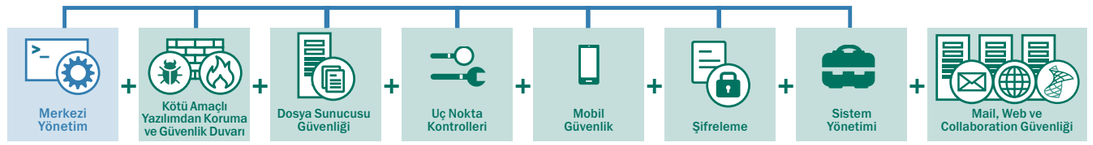
Güçlü Veri Koruması — Uç noktalara Dosya/Klasör (FLE) ve Tam Disk (FDE) şifreleme uygulanabilir. "Taşınabilir mod" desteği, yönetim etki alanlarından ayrılan cihazlar için şifreleme yönetimi sağlar.

Esnek Kullanıcı Oturum Açma — Daha fazla güvenlik için ön yükleme öncesi kimlik doğrulama (PBA), kullanıcı şeffaflığı sağlayan isteğe bağlı "tek oturum açma" özelliğini sunar. 2 kademeli veya belirteç tabanlı kimlik doğrulaması kullanılabilir.

Entegre İlke Oluşturma — Uygulama ve cihaz kontrolleriyle benzersiz şifreleme entegrasyonu, gelişmiş güvenlik sağlayan ve yönetimi kolaylaştıran bir katman ekler

Kaspersky Endpoint Security for Business — ADVANCED seçeneği SELECT ve CORE katmanlarının tüm bileşenlerini içerir.

▶ KASPERSKY TOTAL SECURITY FOR BUSINESS



Tüm BT ortamları için kapsamlı güvenlik isteyen kuruluşlar, Kaspersky Total Security for Business çözümünü seçebilir

Kaspersky Total Security for Business sektörde sunulan en eksiksiz koruma ve yönetme platformunu sağlar. Kaspersky Total Security for Business, ağınızın her katmanını korur ve cihaz — konum ayrımı yapmaksızın kullanıcılarınızın üretken olduğundan ve kötü amaçlı yazılım tehdidinden uzak olduğundan emin olmanızı sağlayacak güçlü yapılandırma araçları içerir.

POSTA SUNUCUSU GÜVENLİĞİ

Olağanüstü yakalama oranları ve minimum hatalı tespit için e-posta tabanlı kötü amaçlı yazılım tehditleri, kimlik avı saldırıları ve spam kullanan bulut tabanlı, gerçek zamanlı güncellemeler. IBM® Domino® için kötü amaçlı yazılımdan koruma dahildir. Microsoft Exchange için DLP işlevi ayrı olarak sunulur.

INTERNET AĞ GEÇİTLERİ İÇİN GÜVENLİK

HTTP(S)/FTP/SMTP ve POP3 trafiğindeki kötü amaçlı ve zarar verme olasılığı taşıyan programları otomatik olarak silerek kuruluş için güvenli internet erişimi sağlar.

İŞ BİRLİĞİ GÜVENLİĞİ

SharePoint® sunucularını ve grupları tüm kötü amaçlı yazılımlara karşı korur. Ayrı olarak sunulan Sharepoint için DLP işlevi, gizli verileri belirleyen ve veri sızıntılarına karşı koruma sağlayan içerik ve dosya filtreleme olanakları sunar.

Kaspersky Total Security for Business ADVANCED, SELECT ve CORE katmanlarının tüm bileşenlerini içerir.

ÜRÜN ÖZELLİKLERİ

Sizin için en uygun çözüm hangisi?

	Core	Select	Advanced	Total	Security Center tarafından yönetilir	Hedeflenmiş Bir Çözümde mevcuttur
Kötü Amaçlı Yazılımdan Koruma	●	●	●	●	●	
Güvenlik Duvarı	●	●	●	●	●	
Uygulama Kontrolü		●	●	●	●	
Cihaz Kontrolü		●	●	●	●	
Web Kontrolü		●	●	●	●	
Dosya Sunucusu Güvenliği		●	●	●	●	●
Mobil Uç Nokta Koruması		●	●	●	●	●
Mobil Cihaz/Uygulama Yönetimi		●	●	●	●	●
Şifreleme			●	●	●	
Güvenlik Açığı Taraması			●	●	●	●
Yama Yönetimi			●	●	●	●
Envanterler			●	●	●	●
Lisans Kontrolü			●	●	●	●
Yazılım Dağıtımı			●	●	●	●
İşletim Sistemi Dağıtımı			●	●	●	●
Collaboration Server Güvenliği				●		●
Posta Sunucusu Güvenliği				●	●	●
Internet Ağ Geçidi Güvenliği				●		●
Sanal Altyapı Güvenliği					●	●
Depolama Sunucusu Güvenliği					●	●

● Dahil ● Kısmen dahil — ayrıntılar için ürün sayfalarına bakın

KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server, sistem performansında fark edilebilir bir etkiye neden olmadan paylaşımlı dosya depolaması için uygun maliyetli, güvenilir ve ölçeklenebilir güvenlik sağlar.

ÖNE ÇIKAN NOKTALAR

GÜÇLÜ KÖTÜ AMAÇLI YAZILIMDAN KORUMA
Kaspersky'nin ödüllü kötü amaçlı yazılımdan koruma motoru, en yeni bilinen ve potansiyel kötü amaçlı yazılım tehditlerinin kötü amaçlı ya da tehlikeli programlar aracılığıyla yerel ağa girmesini engelleyerek güçlü sunucu koruması sağlar.

YÜKSEK PERFORMANS VE GÜVENİLİRLİK
Kaspersky Security for File Server'ın sisteminizi fark edilir şekilde yavaşlatmayacağından veya ağır ağ yükü koşullarında bile kurumsal işlemleri engellemeyeceğinden emin olabilirsiniz.

BİRDEN ÇOK PLATFORM DESTEĞİ
Terminal, küme ve sanal sunucular dahil olmak üzere en yeni platformları ve sunucuları uyumluluk sorunu olmadan destekleyen, heterojen sunucu ağları için tek ve etkili bir güvenlik çözümü.

GÜÇLÜ YÖNETİM VE RAPORLAMA
Etkili, kullanıcı dostu yönetim araçları, sunucu koruma durumuyla ilgili bilgiler, taramalar için esnek saat ayarları ve kapsamlı raporlama sistemi, dosya sunucusu güvenliği için verimli kontrol sağlayarak sahip olma maliyetinin azaltılmasına yardımcı olur.

ÖZELLİKLER

- **En yeni Windows®** (Windows Server® 2012/R2 dahil), Linux® ve FreeBSD (her ikisi için de Samba dahil) sürümlerini çalıştıran dosya sunucuları için gerçek zamanlı kötü amaçlı yazılımdan koruma.
- **Citrix ve Microsoft® terminal sunucu koruması.**
- **Küme sunucuları tamamen destekler.**
- **Ölçeklenebilirlik** — En karmaşık ve heterojen altyapılarda bile kolaylıkla destek ve güvenlik sağlar.
- **Güvenilirlik, kararlılık ve yüksek hata toleransı.**
- **Optimize edilmiş, akıllı tarama teknolojisi,** talep üzerine ve kritik sistem bölgeleri taraması dahil.
- **Güvenilir bölgeler** tarama için kaynak seviyelerini azaltırken güvenlik performansının artmasına yardımcı olurlar.
- Temizleme veya silme öncesinde veriyi **Karantina Altına Alma ve Yedekleme**.
- Virüslü iş istasyonu **izolasyonu**.
- Esnek yapılandırma seçenekleriyle **merkezi kurulum, yönetim ve güncellemeler.**
- **Esnek olay müdahale senaryoları.**
- Ağ koruma durumuna ilişkin **kapsamlı raporlar.**
- **Uygulama durumu bildirim sistemi.**
- **Hiyerarşik Depolama Yönetimi** (HSM) sistemlerine **yönelik destek.**
- **Kanıtlanmış Hyper-V ve Xen Desktop desteği.**
- **VMware ile kullanılabilir.**
- **ReFS desteği.**

Kaspersky Security for File Server, Kaspersky Endpoint Security for Business — SELECT ve ADVANCED'in yanı sıra Kaspersky Total Security for Business'e dahildir. Bu çözüm ayrı bir hedeflenmiş çözüm olarak da satın alınabilir.

UÇ NOKTA KONTROLLERİ TEKNOLOJİMİZ HAKKINDA

En gelişmiş kötü amaçlı yazılımdan koruma ve sektördeki tek Beyaz Liste laboratuvarıyla sıkı şekilde entegre edilen güçlü uç nokta kontrol araçları, işletmenizi bugünün dinamik tehdit ortamında korumanıza yardımcı olur.

KORUYUN, UYGULAYIN, KONTROL EDİN

- Güvenilir uygulamalardaki güvenlik açıkları, web tabanlı kötü amaçlı yazılımlar ve çevre birimleri üzerinde kontrol eksikliği, giderek daha karmaşık hale gelen tehdit ortamının bir parçası olmuştur. Kaspersky Lab'ın Uygulama, Web ve Cihaz Kontrolü araçları, uç noktalarınız üzerinde verimlilikten ödün vermeden kontrol sağlamanıza olanak tanır.

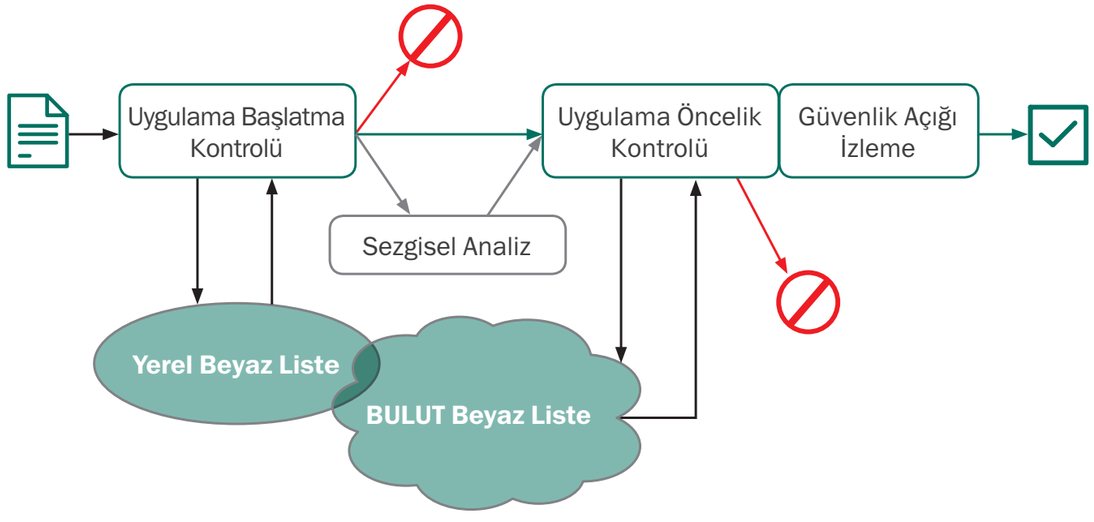
UYGULAMA KONTROLÜ VE DİNAMİK BEYAZ LİSTE

Yöneticilerin uç noktalarda çalıştırılmasına izin verilen uygulamalar ve programlar üzerinde son kullanıcı davranışından bağımsız olarak tam kontrole sahip olmasını sağlayarak sistemlerinizi bilinen ve bilinmeyen tehditlere karşı koruyun. Ayrıca, uygulamanın davranışını değerlendirmek ve uygulama veya ağ için tehlike oluşturabilecek beklenmedik eylemler gerçekleştirmesini önlemek için uygulama bütünlüğü izleme özelliğini etkinleştirin. Basitleştirilmiş, özelleştirilebilir ve otomatik ilke oluşturma ve uygulama şunlara olanak sağlar:

- **Uygulama başlatma kontrolü**: Uygulama başlatma izni verme, engelleme ve denetleme. İşle ilgili olmayan uygulamalara erişimi kısıtlayarak verimliliği artırın.
- **Uygulama ayrıcalık kontrolü**: Uygulamanın sistem kaynakları ve verilerine erişimini düzenleyin ve kontrol edin. Uygulamaları, güvenilir, güvenli olmayan veya kısıtlı etiketleriyle sınıflandırın. Uygulamanın uç noktalarda web tarayıcısı veya Skype tarafından gönderilen bilgiler gibi şifrelenmiş verilere erişimini yönetin.
- **Uygulama güvenlik açığı taraması:** Saldırılara karşı proaktif savunma, güvenilir uygulamalardaki güvenlik açıklarını hedef alır.

Kontrol çözümlerinin büyük bölümü sadece temel engelleme/erişim işlevleri sunar. Kaspersky Lab'ın kontrol araçları, bulut tabanlı beyaz liste veritabanlarını kullanarak ve en yeni uygulama verilerine neredeyse gerçek zamanlı erişim sağlayarak benzersiz koruma sunar.

Kaspersky Lab'ın uygulama kontrol teknolojileri uygulamaları indirme, yükleme ve çalıştırma düzeylerinde analiz etmek ve izlemek için bulut tabanlı beyaz liste veritabanlarını kullanır.



Dinamik Beyaz Liste, yöneticiler tarafından kesin bir şekilde izin verilmediği sürece tüm iş istasyonlarında aktif hale gelmeye çalışan uygulamaların hepsini engelleyen, kapsamlı "Varsayılan Olarak Reddet" seçeneğiyle etkinleştirilebilir.
Kaspersky Lab, 500 milyondan fazla programı sürekli olarak gözlem altında tutan ve güncel veritabanları sunan özel Beyaz Liste laboratuvarına sahip olan tek güvenlik şirketidir.

Kaspersky Lab'ın **Varsayılan Olarak Reddet seçeneğinin test ortamında uygulanabilmesi**, yöneticilerin uygulamayı engellemeden önce yasal olup olmadığını belirlemelerine olanak sağlar. Ayrıca, dijital imza tabanlı uygulama kategorilerinin oluşturulabilmesi, kullanıcıların kötü amaçlı yazılım tarafından değişikliğe uğratılan veya şüpheli bir kaynaktan gelen yasal yazılımları çalıştırmasını önler.

KOLAY YÖNETİM

Tüm Kaspersky Lab kontrol araçlarının Active Directory ile entegre olması, genel ilkelerin basit ve hızlı şekilde ayarlanmasını sağlar. Tüm uç nokta kontrolleri, aynı konsoldan tek bir arabirim kullanılarak yönetilebilir.

WEB KONTROLLERİ

Son kullanıcının işyerinde erişebildiği web sitelerinin izlenmesi, filtrelenmesi ve kontrol edilmesi, verimliliği artırmanın yanı sıra web tabanlı kötü amaçlı yazılım ve saldırılara karşı koruma sağlar.

Kaspersky Lab'ın gelişmiş web kontrolleri, anlık olarak güncellenen ve kategorilere ayrılan (örn. yetişkin, oyun, sosyal ağ, kumar) bir web siteleri dizininde oluşturulur. Yöneticiler son kullanıcıların bireysel siteleri kullanmalarını önleyen, sınırlayan veya denetleyen ilkeleri kolayca oluşturabilir ve kendi listelerini hazırlayabilirler. Kötü amaçlı siteler otomatik olarak engellenir.

Kaspersky Lab'ın web kontrolleri, sosyal ağlar ve anlık mesaj servislerinin kullanımını kısıtlayarak bu uygulamalardan kaynaklanan veri kayıplarının önlenmesine yardımcı olur. Esnek ilkeler, yöneticilerin İnternet kullanımına günün belirli saatlerinde izin vermelerine olanak sağlar. Active Directory entegrasyonu sayesinde ilkeler kuruluş genelinde hızlı ve kolay şekilde uygulanabilir.

Kaspersky Lab'ın web kontrolleri, daha fazla güvenlik için doğrudan uç noktada etkinleştirilebilir ve ilkelerin çalışanların ağda olmadığı durumlarda da uygulanması sağlanabilir.

CİHAZ KONTROLLERİ

USB bağlantı noktasının devre dışı bırakılması, çıkarabilir cihaz sorunlarını her zaman ortadan kaldırmaz. Örneğin; USB bağlantı noktasının devre dışı bırakılması, belirteç tabanlı VPN erişimi gibi diğer güvenlik önlemlerini etkileyebilir.

Kaspersky Lab'ın cihaz kontrolleri, veriyolu, cihaz türü ve cihaz kimliği düzeyinde daha parçalı bir kontrol seviyesi sağlayarak güvenliği optimize eder ve son kullanıcı verimliliğini korur. Kontroller doğrudan cihazın özgün seri numarasına uygulanabilir.

- Cihazlar için bağlanma/okuma/yazma izinlerinin yanı sıra zaman planlaması ayarlayın.
- Maskelere dayalı cihaz kontrolü kuralları oluşturarak cihazların beyaz listeye alınmasına izin vermek için fiziksel bağlantı gereksinimini ortadan kaldırın. Birden fazla cihazı eşzamanlı olarak beyaz listeye dahil edin.
- Çıkarılabilir cihazlardaki veri değişimini kuruluş içinde ve dışında kontrol ederek veri kaybı veya hırsızlığı riskini azaltın.
- Belirli cihaz türlerine şifreleme ilkeleri uygulamak için Kaspersky Lab'ın şifreleme teknolojileriyle entegre edin.

Uç Nokta Kontrolleri teknolojisi, Kaspersky Endpoint Security for Business — SELECT ve ADVANCED'in yanı sıra Kaspersky Total Security for Business'e dahildir.

KASPERSKY SECURITY FOR MOBILE

Mobil cihazlar gün geçtikçe siber suçlulara daha çekici gelmektedir. Bununla birlikte, "Kendi Cihazını Getir" (BYOD) yaklaşımı cihaz yelpazesini daha çeşitli ve karmaşık hale getirerek, BT yöneticileri için zorlu bir yönetim ve kontrol ortamı ortaya çıkarmaktadır.

Kaspersky Security for Mobile cihazınızın her yerde güvende olmasını sağlar. Sürekli gelişen kötü amaçlı mobil yazılımlara karşı koruma sağlayın. Ortamınızdaki akıllı telefonlar ve tabletler üzerinde tek bir merkezi konumdan ve minimum müdahale ile hızlı ve kolay görünürlük ve kontrol sağlayın.

TEMEL ÜRÜN ÖZELLİKLERİ

- **Güçlü Kötü Amaçlı Yazılımdan Koruma**
- **Kimlik Avı Koruması ve Anti-spam**
- **Web koruması**
- **Uygulama Kontrolü**
- **Rooting/jailbreak algılaması**
- **Konteynerizasyon**
- **Hırsızlığa karşı koruma**
- **Mobil Cihaz Yönetimi**
- **Self Servis Portal**
- **Merkezi yönetim**
- **Web Konsolu**
- **Desteklenen platformlar:**
  - **Android™**
  - **iOS**
  - **Windows® Phone**

ÖNE ÇIKAN NOKTALAR

MOBİL CİHAZLAR İÇİN GELİŞMİŞ KÖTÜ AMAÇLI YAZILIMDAN KORUMA VE VERİ GÜVENLİĞİ
Sadece 2014 yılında, Kaspersky Lab yaklaşık 1,4 milyon benzersiz mobil kötü amaçlı saldırıyı önledi. Kaspersky Security for Mobile, mobil cihazlarda saklanan verileri bilinen ve bilinmeyen tehditlere karşı koruyan kötü amaçlı yazılım önleme ve derin koruma teknolojisi katmanlarını bir arada kullanır.

MOBİL CİHAZ YÖNETİMİ (MDM)
Tüm lider mobil cihaz yönetim platformlarıyla entegrasyon, Android, iOS ve Windows Phone cihazlarının daha kolay kullanılabilmesi ve yönetilebilmesi için uzaktan "Kablosuz" (OTA) dağıtım ve kontrol olanağı sağlar.

MOBİL UYGULAMA YÖNETİMİ (MAM)
Konteynerizasyon ve seçmeli silme olanakları aynı cihazda işletme verileri ve kişisel verilerin ayrılmasına olanak sağlayarak BYOD girişimlerini destekler. Şifreleme işlevimiz ve kötü amaçlı yazılımdan koruma teknolojimizle birlikte kullanılan Kaspersky Security for Mobile, cihazı ve verilerini yalıtarak korumayı deneyen basit bir çözüm değil, bir proaktif mobil koruma çözümüdür.

MERKEZİ YÖNETİM
Birden fazla platform ve cihazı aynı konsoldan farklı uç noktaları olarak yönetin. Bu platform, daha fazla çaba veya teknoloji yönetimi gereksinimi ortaya çıkarmadan görünürlüğü ve kontrolü artırır.

MOBİL GÜVENLİK VE YÖNETİM ÖZELLİKLERİ

GÜÇLÜ KÖTÜ AMAÇLI YAZILIMDAN KORUMA
İmza tabanlı, proaktif ve bulut destekli (Kaspersky Security Network — KSN ile) koruma bilinen ve bilinmeyen mobil kötü amaçlı tehditlere karşı koruma sağlar. İsteğe bağlı ve planlı taramalar ve otomatik güncellemeler koruma düzeyini artırır.

KİMLİK AVI KORUMASI VE ANTİ-SPAM
Güçlü Kimlik Avı Koruması ve Anti-Spam teknolojileri, cihazı ve verileri kimlik avı saldırılarına karşı korur ve istenmeyen çağrı ve mesajların filtrelenmesine yardımcı olur.

WEB KONTROLÜ/SAFE BROWSER
Kaspersky Security Network (KSN) tarafından desteklenen bu teknolojiler, kötü amaçlı ve izinsiz kullanımı hedefleyen web sitelerinin erişimini engellemek için gerçek zamanlı olarak çalışırlar. Safe Browser sürekli güncellenen itibar analizi sunarak güvenli mobil gezinme sağlar.

UYGULAMA KONTROLÜ
KSN ile entegre edilen Uygulama Kontrolü, uygulamanın sadece onaylı yazılımı kullanmasını sağlayarak belirsiz veya izinsiz yazılımların kullanılmasını önler. Cihaz işlevini gerekli uygulamaların yüklenmesine bağlı hale getirin. Uygulama etkin olmama kontrolü, yöneticilerin uygulamaların belirli bir süre boyunca kullanılmadığı durumlar için yeniden oturum açmayı zorunlu kılmasına olanak sağlar. Bu yaklaşım cihaz kaybolduğunda veya çalındığında uygulama açık olsa bile verilerin korunmasını sağlar.

ROOTING/JAILBREAK ALGILAMASI
Rooting veya jailbreak işlemlerini otomatik algılama ve raporlama, konteynerlere erişimi otomatik engelleme, seçmeli silme veya tüm cihazı silme özellikleriyle takip edilebilir.

KONTEYNERİZASYON
Uygulamaları konteynerlerde "paketleyerek" işletme verilerini ve kişisel verileri birbirinden ayırın. Hassas verileri korumak için şifreleme gibi ek ilkeler uygulanabilir. Seçmeli silme, işletmeden ayrılan çalışanın cihazında konteynerde saklanan verilerin çalışanın kişisel verilerine dokunmadan silinmesine olanak sağlar.

HIRSIZLIĞA KARŞI KORUMA
Silme, cihazı kilitleme, konum belirleme, SIM izleme, "gizli fotoğraf çekme" ve "alarm" cihazı algılama gibi uzaktan Hırsızlığa Karşı Koruma özellikleri, cihazın kaybolduğu ya da çalındığı durumlarda etkinleştirilebilir. Hırsızlığa karşı koruma komutları, duruma bağlı olarak oldukça esnek bir şekilde uygulanabilir. Örneğin, Google Cloud Messaging (GCM) entegrasyonu komutların anında iletilmesini sağlar, yanıt sürelerini kısaltır ve güvenliğe katkıda bulunur. Ayrıca komutların Self-Service Portal ile gönderilmesi yöneticilerin eyleme geçmesi zorunluluğunu ortadan kaldırır.

MOBİL CİHAZ YÖNETİMİ (MDM)
Microsoft® Exchange ActiveSync, Apple MDM ve Samsung KNOX 2.0 desteği, geniş bir ilke kapsamını birleşik bir arabirimle ve platformdan bağımsız olarak etkinleştirir. Örn. şifreleme ve parola uygulama veya kamera kullanımı kontrol etme, bireysel kullanıcılar ya da gruplara ilkeler uygulama, APN/VPN ayarlarını yönetme vb.

SELF SERVİS PORTAL
Rutin güvenlik yönetiminin çalışanlara dağıtılması, onaylı cihazların otomatik kaydedilmesini sağlar. Yeni cihaz etkinleştirme sürecinde tüm gerekli sertifikalar, yönetici müdahalesine gerek olmadan portal üzerinden otomatik olarak gönderilebilir. Cihazın kaybolması durumunda, çalışan tüm mevcut Hırsızlığa Karşı Koruma eylemlerini Portal yoluyla uygulayabilir.

MERKEZİ YÖNETİM
Tüm mobil cihazları, aynı zamanda tüm diğer uç noktaların BT güvenliğinin yönetilmesine olanak sağlayan tek bir konsoldan merkezi olarak yönetin. Web Konsolu, yöneticilerin cihazları tüm bilgisayarlardan uzaktan kontrol etmelerine ve yönetmelerine olanak sağlar.

Kaspersky Security for Mobile, Kaspersky Endpoint Security for Business — SELECT ve ADVANCED'in yanı sıra Kaspersky Total Security for Business'e dahildir. Bu çözüm ayrı bir hedeflenmiş çözüm olarak da satın alınabilir.

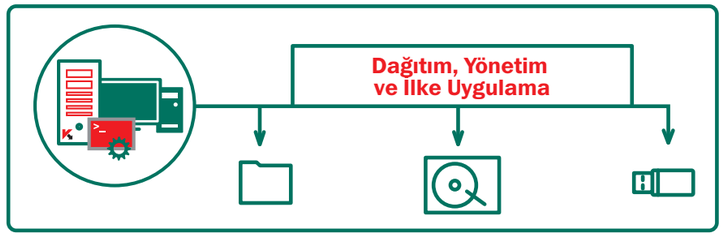
ŞİFRELEME TEKNOLOJİMİZ HAKKINDA

Cihazın kaybolması, hırsızlık veya veri çalmaya yönelik kötü amaçlı yazılımların neden olduğu yetkisiz veri erişimini önler.

Proaktif veri koruması ve uyumluluk, küresel ölçekte bir gerekliliktir. Kaspersky Lab'ın şifreleme teknolojisi, değerli verileri kaza sonucu kaybolma, cihaz hırsızlığı ve hedefli saldırılarda kullanılan kötü amaçlı yazılımlara karşı korur. Güçlü şifreleme teknolojisini Kaspersky Lab'ın sektör lideri uç nokta koruma teknolojileriyle bir arada kullanan entegre platformumuz, verileri saklanırken ve taşınırken korur.

Kaspersky Lab tarafından üretilen bu teknoloji, kolayca uygulanabilir ve merkezi bir yönetim konsolundan tek bir ilke kullanılarak yönetilebilir.

Kaspersky Lab Şifreleme Teknolojisi ile veri kaybını ve bilgilerinize izinsiz erişimi önleyin:
- **Tam Disk Şifreleme (FDE)**
- **Dosya/Klasör Düzeyi (FLE)**
- **Çıkarılabilen ve Yerleşik Cihazlar**



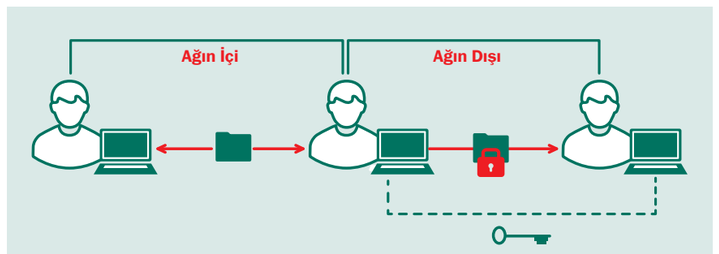
TEK BİR YÖNETİM KONSOLUYLA YÖNETİLİR

SEKTÖR STANDARDI GÜVENLİ ŞİFRELEME
Kaspersky Lab, basitleştirilmiş anahtar yönetimi ve emanet olarak saklama özelliklerine sahip 256 bit uzunluğunda anahtarlardan faydalanan Gelişmiş Şifreleme Standardı'nı (AES) kullanır. Intel® AES-NI teknolojisini, UEFI ve GPT platformlarını destekler.

TAM ESNEKLİK
Kaspersky Lab, dosya ve klasör düzeyinde şifreleme (FLE) ve tam disk şifreleme (FDE) sunarak tüm olası kullanım senaryolarında koruma sağlar. Sabit sürücüler ve taşınabilir cihazlardaki veriler korunabilir. "Taşınabilir mod", verilerin şifreleme yazılımı yüklenmemiş bilgisayarlarda bile şifrelenmiş taşınabilir ortamda kullanılmasını ve aktarılmasını sağlayarak "tesis dışı" veri değişimlerinin güvenle gerçekleştirilmesini kolaylaştırır.

TEK OTURUM AÇMA VE SON KULLANICI ŞEFFAFLIĞI
Kaspersky Lab'ın şifreleme teknolojisi, kurulumdan günlük kullanıma kadar tüm uygulamalarda kullanıcı verimliliğini sekteye uğratmadan şeffaf şekilde çalışır. Sorunsuz şifreleme sağlayan tek oturum açma son kullanıcının teknolojinin çalıştığını bile fark etmeden korunmasını sağlar.

Kaspersky Lab'ın şifrelemesi ağ içindeki ve dışındaki kullanıcılar arasında sorunsuz, şeffaf dosya aktarımına olanak sağlar.



ŞİFRELEME ÖZELLİKLERİ

KASPERSKY LAB GÜVENLİK TEKNOLOJİLERİYLE SORUNSUZ ENTEGRASYON
Genel kod tabanında yerleşik çok katmanlı güvenlik için Kaspersky Lab kötü amaçlı yazılımdan koruma, uç nokta kontrolleri ve yönetim teknolojileriyle tam entegrasyon. Örneğin, belirli çıkarılabilir cihazlarda şifreleme tek bir ilke ile yönetilebilir. Şifreleme ayarlarını kötü amaçlı yazılımdan koruma, cihaz kontrolü ve diğer uç nokta güvenlik bileşenlerine aynı ilke altında uygulayın. Farklı çözümler uygulama ve yönetme gerekliliğini ortadan kaldırır. Ağ donanımı uyumluluğu şifreleme uygulanmadan önce otomatik olarak kontrol edilir; UEFI ve GPT platformlarına standart olarak destek sunulur.

ROL TABANLI ERİŞİM KONTROLÜ
Büyük ölçekli kuruluşlarda, rol tabanlı erişim işlevini kullanarak şifreleme yönetimini yetkilere göre sınıflandırmayı seçin. Bu yaklaşım daha az karmaşık bir şifreleme yönetimine olanak sağlar.

ÖNYÜKLEME ÖNCESİ KİMLİK DOĞRULAMA (PBA)
İsteğe bağlı tek oturum açma platformunda işletim sistemi önyüklenmeden önce kimlik bilgilerinin girilmesi zorunlu hale getirilerek bir ek güvenlik katmanı sağlanır. Kaspersky Lab'ın şifreleme teknolojisi PBA, ayrıca QWERTY dışındaki klavye yerleşimlerinde de kullanılır.

AKILLI KART VE BELİRTEÇLE KİMLİK DOĞRULAMA
Akıllı kartlar ve belirteçlerin sık kullanılan tasarımlarıyla İki Kademeli Kimlik Doğrulamayı destekler, ek kullanıcı adı ve parola gereksinimi ortadan kaldırır ve kullanıcı deneyimini geliştirir.

ACİL DURUM KURTARMA
Yöneticiler donanım veya yazılım arızası durumunda verileri şifreleyebilir. PBA için kullanıcı parolası kurtarma veya şifrelenmiş veri erişimi, basit bir soru-cevap mekanizmasıyla uygulanabilir.

OPTİMİZE DAĞITIM, ÖZELLEŞTİRİLEBİLEN AYARLAR
Kaspersky Lab'ın şifreleme işlevi, dağıtım kolaylığı amacıyla ayrı kurulum gereksinimini ortadan kaldıracak şekilde sadece Kaspersky Endpoint Security for Business'ın "Advanced" ve "Total" katmanlarında etkinleştirilir. Şifreleme ayarları önceden belirlenmiş olmasına karşın Belgelerim, Masaüstü gibi sık kullanılan klasörler, yeni klasörler, dosya uzantıları ve Microsoft® Office belgeleri veya mesaj arşivleri gibi gruplar için özelleştirilebilir.

Şifreleme Kontrolleri teknolojisi, Kaspersky Endpoint Security for Business — ADVANCED'in yanı sıra Kaspersky Total Security for Business'e dahildir.

KASPERSKY SYSTEMS MANAGEMENT

Merkezi BT yönetim araçlarıyla güvenliği artırın ve karmaşıklığı azaltın.

Popüler uygulamalarda yama uygulanmayan güvenlik açıkları, işletme BT güvenliğine yönelik en önemli tehditlerden biridir. Sahip olduğunuz cihazlarını tanımadığınızda ve nasıl koruyacağınızı bilmediğinizde BT karmaşıklığının artması riskin artması anlamına gelebilir.

Güvenlik açığı değerlendirmesi, yama ve güncelleme dağıtımı, envanter yönetimi ve uygulama sunumları gibi temel güvenlik, yapılandırma ve yönetim görevlerini merkezi ve otomatik hale getirmek sadece zamandan tasarruf etmenizi sağlamakla kalmaz aynı zamanda güvenliği optimize eder.

BT güvenlik risklerinin en aza indirilmesine yardımcı olan ve BT karmaşıklığını azaltan Kaspersky Systems Management, yöneticilerin birçok cihaz, uygulama ve kullanıcı üzerinde tek bir ekrandan eksiksiz, gerçek zamanlı kontrol ve görünürlük sağlamasına imkan tanır.

TEMEL ÜRÜN ÖZELLİKLERİ

- **Güvenlik Açığı Taraması ve Yama Yönetimi**
- **Donanım ve yazılım envanterleri**
- **Uzak ofis gereksinimleri dahil olmak üzere uzaktan yazılım yükleme ve sorun giderme**
- **İşletim sistemi dağıtımı**
- **SIEM entegrasyonu**
- **Rol tabanlı erişim kontrolü**
- **Merkezi yönetim**

GÜVENLİĞİ ARTIRIN

Planlı, otomatik yamalar ve güncellemelerle BT güvenliğini artırın ve rutin görevleri azaltın. Otomatik güvenlik açığı keşfetme ve öncelik belirleme, verimliliğin artmasına katkıda bulunur ve kaynak yükünü azaltır. Bağımsız testler[1] Kaspersky Lab'ın en kısa sürede en kapsamlı otomatik yama ve güncelleme kapsamını sağladığını göstermektedir.

TAM GÖRÜNÜRLÜKLE KONTROL SAĞLAYIN

Tek bir konsoldan sağlanan tam ağ görünürlüğü, tahmine dayalı yönetimi ortadan kaldırır ve ağa giren her bir uygulama ve cihaz hakkında (konuk cihazlar dahil) bilgi sahibi olmanızı sağlar. Bu yaklaşım, kuruluşun verilerine ve uygulamalarına erişen kullanıcı ve cihazların merkezi olarak ve BT ilkeleriyle uyumlu şekilde kontrol edilmesine imkan tanır.

MERKEZİ OLARAK YÖNETİN

Kaspersky Lab Systems Management, Kaspersky Security Center'dan yönetilebilen bir bileşendir. Rutin BT görevlerini otomatik hale getirmek için tutarlı, sezgisel komutlar ve arabirimler kullanılır. Bu platform her bir özelliği merkezi konsoldan erişilebilir ve yönetilebilir hale getirir.

ÖZELLİKLER

GÜVENLİK AÇIĞI TARAMASI VE YAMA YÖNETİMİ

Otomatik yazılım taraması, güvenlik açıklarının hızlı şekilde algılanmasına, önceliğinin belirlenmesine ve iyileştirilmesine olanak sağlar. Microsoft® ve Microsoft dışı yazılımlar için yamalar ve güncellemeler en kısa zaman aralıklarıyla[2] otomatik olarak sağlanır. Yöneticiler yama yükleme durumu hakkında bilgilendirilir.

Büyük önem taşımayan düzeltmeler çalışma saatleri sonrasına ertelenerek, bilgisayarlar kapalı olsa bile LAN uyanması yoluyla gerçekleştirilebilir. Multicast yayın, yamaların ve güncellemelerin uzak ofislere yerel olarak dağıtılmasını sağlayarak, bant genişliği gereksinimini azaltır.

DONANIM VE YAZILIM ENVANTERLERİ

Çıkarılabilir cihazlar dahil olmak üzere donanım ve yazılımın otomatik keşfedilmesi, envantere alınması, bildirilmesi ve izlenmesi, yöneticilere kurumsal ağda kullanılan cihazlar ve varlıklara yönelik ayrıntılı bilgi sağlar. Konuk cihazlar algılanabilir ve bu cihazlara İnternet erişimi sağlanabilir. Lisans kontrolü, birçok düğüm ve son kullanma tarihi hakkında görünürlük sağlar.

ESNEK İŞLETİM SİSTEMİ VE UYGULAMA SUNMA

Merkezi, kolay oluşturulan, depolanan, klonlanan ve dağıtılan optimum güvenliğe sahip sistem görüntüleri. Yükleme sonrası düzenleme özellikli LAN Uyanması ile çalışma saatleri sona erdiğinde dağıtma olanağı mükemmel esneklik sağlar. UEFI desteği.

YAZILIM DAĞITIMI

Yazılımları tek bir konsoldan uzaktan dağıtın/güncelleyin. Kaspersky Security Network tarafından tanınan 100'ün üzerinde popüler uygulama, isteğe bağlı olarak çalışma saatlerinden sonra otomatik olarak yüklenebilir. Kullanıcı izinleri ve oturum günlükleri/denetimleriyle gelişmiş güvenlik özellikleri sunan uzaktan sorun gidermeye yönelik tam destek. Yerel yazılım dağıtımı gerçekleştiren Multicast teknolojisi sayesinde uzak ofis trafiğini azaltın.

SIEM ENTEGRASYONU

IBM® QRadar ve HP ArcSight gibi lider SIEM sistemlerine doğrudan raporlama ve olay aktarımı kontrolü. Günlükler ve diğer güvenlikle ilgili verilerin analiz amacıyla toplanması, yönetim iş yükü ve araçları en aza indirmenin yanı sıra kurumsal düzeyde raporlamayı basitleştirir.

ROL TABANLI ERİŞİM KONTROLÜ

Karmaşık ağlarda yönetim rollerini ve sorumluluklarını dağıtın. Konsol görünümünü roller ve haklara göre özelleştirin.

MERKEZİ YÖNETİM

Kaspersky Security Center'ın tek entegre yönetim konsolu, masaüstü bilgisayar, mobil cihaz ve sanal uç nokta güvenliğinin ağ boyunca tek bir arabirimden yönetilmesini destekler.

Kaspersky Systems Management, Kaspersky Endpoint Security for Business — ADVANCED'in yanı sıra Kaspersky Total Security for Business platformuna dahildir. Bu çözüm ayrı bir Hedeflenmiş Çözüm olarak da satın alınabilir.

1, 2 Yama Yönetim Çözümleri Testi Kaspersky Lab tarafından finanse edilmiş ve AV-TEST GmbH tarafından gerçekleştirilmiştir (Temmuz 2013)

► KASPERSKY SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server, en karmaşık heterojen altyapılarda bile posta sunucularındaki trafik için spam, kimlik avı ve hem genel hem de gelişmiş kötü amaçlı yazılım tehditlerine karşı olağanüstü koruma sağlar.

E-posta ve eklerden kaynaklanan gizli veri kayıplarına karşı koruma ayrıca Microsoft® Exchange Server Ortamları için sağlanır.

ÖNE ÇIKAN NOKTALAR

KÖTÜ AMAÇLI YAZILIM TEHDİTLERİNE KARŞI KORUMA
Proaktif girişim koruması ve kötü amaçlı URL filtreleme özelliğiyle birlikte sunulan kötü amaçlı yazılımlara karşı güçlü koruma, Kaspersky'nin ödüllü kötü amaçlı yazılımdan koruma motoru tarafından sağlanır, bulut yardımlı Kaspersky Security Network tarafından gerçek zamanlı olarak desteklenir.

ANTİ-SPAM KORUMASI
Microsoft Exchange ve Linux® tabanlı posta sunucularında, Kaspersky'nin bulut yardımlı anti-spam motorunun zaman ve kaynak tüketen spam mesajları minimum hatalı tespitle %99,96'ya varan bir oranla engellediği kanıtlanmıştır.

VERİ KAYBI KORUMASI VE KONTROL (MICROSOFT EXCHANGE SERVERS)*
İşletme, finans, kişisel ve diğer hassas verilerin Microsoft Exchange sunucularında giden e-postalara ve eklere dahil edildiğini algılayan ve bu bilgilerin akışını kontrol eden Kaspersky Security for Mail Servers, sizin ve çalışanlarınızın gizli verilerinin güvenli şekilde saklanmasını ve veri koruma düzenlemeleriyle uyumlu olmasını sağlar. Yapılandırılmış veri aramaları ve işletmeye özel sözlükler gibi gelişmiş analiz teknikleri şüpheli e-postaların belirlenmesine ve ardından engellenmesine katkıda bulunur. Sistem ayrıca gönderenin Yöneticisini olası güvenlik açıklarına karşı uyarabilir.

BASİT, ESNEK YÖNETİM
Kullanıcı dostu yönetim ve raporlama araçları ve esnek tarama ayarları, posta ve belge güvenliğinizi verimli şekilde kontrol etmenizi sağlayarak toplam sahip olma maliyetinin azaltılmasına yardımcı olur.

ÖZELLİKLER

- Bulut destekli Kaspersky Security Network tarafından desteklenen gerçek zamanlı kötü amaçlı yazılımdan koruma.
- Bilinmeye girişimlere ve hatta sıfır saat güvenlik açıklarına karşı anında koruma.
- Spam'e karşı gelişmiş koruma: Kaspersky Lab'in anti-spam motoru istenmeyen e-posta trafiğinin %99'undan fazlasını engeller.
- Veri Sızıntısı Koruması (Microsoft Exchange Sunucuları)*. E-posta ve eklerdeki gizli bilgileri, kategoriler (kişisel bilgiler ve ödeme kartı verileri dahil), sözlükler ve yapılandırılmış veri kullanan derin seviye analizi yoluyla algılama.
- Genel klasörler dahil olmak üzere Microsoft® Exchange sunucularındaki tüm mesajlar için Kaspersky Security Network kullanılarak yapılan gerçek zamanlı, bulut yardımlı anti-spam taraması.
- E-postalar ve Lotus Domino veritabanları için zamanlanmış tarama.
- IBM® Domino® sunucularındaki mesajlar, veritabanları ve diğer nesnelere yönelik tarama.
- Bilinen ek biçimleri, boyutları ve adlarına göre mesaj filtreleme.
- Kolay ve kullanışlı kötü amaçlı yazılımdan koruma ve anti-spam veritabanı güncelleme işlemi.
- Temizleme veya silme işleminden önce yedek veri depolama.
- Ölçeklenebilirlik ve hata toleransı.
- Kolay kurulum ve esnek entegre yönetim.
- Güçlü bildirim sistemi.
- Ağ koruma durumuna ilişkin kapsamlı raporlar.

*Bu ürün satın alınırken, gizli veri kaybı veya sızıntı önleme seçeneği ayrı olarak satılır.

► KASPERSKY SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway, tüm iş gücünüz için güvenli ve her zaman açık İnternet erişimi sağlayan birinci sınıf bir kötü amaçlı yazılımdan koruma çözümüdür.

ÖNE ÇIKAN NOKTALAR

KAPALI KALMA SÜRESİNİ VE KESİNTİLERİ AZALTAN GÜÇLÜ KORUMA
Kaspersky Labs'in ödüllü kötü amaçlı yazılımdan koruma motoru, en yeni bilinen ve potansiyel kötü amaçlı yazılım tehditlerinin kötü amaçlı veya tehlikeli programlar aracılığıyla yerel ağa girmesini engeller.

OPTİMİZASYON ARACILIĞIYLA PERFORMANS VERİMLİLİĞİ
Optimize edilmiş, akıllı tarama teknolojisi ve yük dengeleme, kaynaklar üzerindeki yükü azaltarak güvenlik performansından ödün vermeden değerli bant genişliğinin korunmasına yardımcı olur.

BİRDEN ÇOK PLATFORM DESTEĞİ
Proxy sunucuları dahil olmak üzere en yeni platformlara ve sunuculara yönelik destek, heterojen ortamlarda ağır ağ trafiği hacimleriyle çalışan kuruluşlar için ideal. Microsoft® Forefront® TMG desteği, kurumsal postanın yanı sıra web ağ geçidi korumasına kadar uzanır.

BASİT YÖNETİM VE RAPORLAMA
Basit ve kullanıcı dostu yönetim araçları, esnek tarama ayarları ve koruma durumu raporlama sistemleri.

ÖZELLİKLER

- Büyümekte olan ve bilinen kötü amaçlı yazılım tehditlerine karşı **her zaman açık, proaktif koruma**.
- Minimum hatalı tespitin yanı sıra **olağanüstü kötü amaçlı yazılım algılama oranları.**
- **Optimize edilmiş, akıllı tarama teknolojisi.**
- Yayınlanmış sunuculardan **gerçek zamanlı HTTP, HTTPS ve FTP trafiği taraması.**
- En popüler Linux proxy sunucusu olan **Squid'e yönelik koruma.**
- Kurulum, yönetim ve güncellemeler için **kullanışlı araçlar.**
- **Esnek tarama araçları ve olay müdahale senaryoları**.
- Sunucu işlemcileri için **yük dengeleme.**
- **Ölçeklenebilirlik ve hata toleransı.**
- Ağ koruma durumuna ilişkin **kapsamlı raporlama.**

MICROSOFT® FOREFRONT® TMG VE ISA SUNUCULARINA ÖZEL ÖZELLİKLER:

- Uygulama durumu için gerçek zamanlı izleme.
- VPN bağlantılarını tarama.
- Gerçek zamanlı HTTPS trafiği taraması (yalnızca TMG).
- E-posta trafiği koruması (POP3 ve SMTP protokolleri üzerinden).
- Yedekleme depolama (yalnızca TMG).

Kaspersky Security for Mail Server ve Kaspersky Security for Internet Gateway, Kaspersky Total Security for Business'e dahildir ve ayrı bir Hedeflenmiş Çözüm olarak da satın alınabilir.

► KASPERSKY SECURITY FOR COLLABORATION

SharePoint ortamları dahil olmak üzere işbirliği platformları için veri koruma ve kontrol.

ÖNE ÇIKAN NOKTALAR

SHAREPOINT PLATFORMUNUZU TAM OLARAK KORUR
Bilinen, bilinmeyen ve gelişmiş tehditlere karşı güçlü koruma bulut destekli Kaspersky Security Network tarafından sağlanırken, kimlik avı koruması teknolojisi işbirliğine dayalı verilere yönelik web tabanlı tehditlere karşı koruma sunar.

GİZLİ VERİ SIZINTISINI ÖNLER*
Önceden yüklenmiş sözlükler ve veri kategorilerini kullanan Kaspersky Security for Collaboration, SharePoint sunucularına kaydedilen tüm belgeleri hassas bilgilere karşı kelime kelime ve ifade ifade kontrol eder.

İLETİŞİM POLİTİKALARI UYGULAR
İçerik ve filtreleme özellikleri, uygunsuz içeriği tanımlayıp engellerken diğer yandan da uygunsuz dosyaların ve dosya biçimlerinin boş yere depolanmasını önleyerek iletişim ilkelerinizi ve standartlarınızı uygulamanıza yardımcı olur.

ÖZELLİKLER

KÖTÜ AMAÇLI YAZILIMDAN KORUMA
- **ERİŞİM SIRASINDA TARAMA** — dosyalar yükleme veya indirme sırasında gerçek zamanlı olarak taranır.
- **ARKA PLANDA TARAMA** — sunucularda saklanan dosyalar en yeni kötü amaçlı yazılımdan koruma imzaları kullanılarak düzenli şekilde kontrol edilir.
- **KASPERSKY SECURITY NETWORK ENTEGRASYONU** — sıfır gün tehditlerinde bile gerçek zamanlı bulut destekli koruma sağlar.

KURULUŞUNUZUN İLETİŞİM İLKELERİNİ DESTEKLER
- **Dosya filtreleme**, belge depolama ilkelerinin uygulanmasına ve depolama cihazlarına yönelik taleplerin azaltılmasına yardımcı olur. Gerçek dosya biçimlerini uzantı adından bağımsız olarak analiz eden uygulama, kullanıcıların güvenlik politikasını ihlal eden dosya türlerini kullanamamasını sağlar.
- **Wiki/blogları koruma,** wikiler ve bloglar dahil olmak üzere tüm SharePoint deposunu korur.
- **İçerik filtreleme,** uygunsuz içeriğe sahip dosyaların depolanmasını önler. Her bir dosyanın içeriği anahtar sözcüklere dayalı olarak analiz edilir. Müşteriler ayrıca kendilerine özgü içerik filtreleme sözlükleri oluşturabilirler.

GİZLİ VERİ KAYBI KORUMASI*
- **Gizli bilgiler için belge tarama**. Çözüm belirli veri türlerini algılayan ve bu verilerin ilgili yasal standartları karşıladığını onaylayan modüllerle entegre olur. Örneğin, kişisel veriler (HIPAA veya AB Direktifi 95/46EC gibi uyumluluk düzenlemeleri tarafından tanımlanır) ya da PCI DSS standart verileri (Ödeme Kartı Sektör Veri Güvenliği Standardı). Veriler yerleşik, düzenli olarak güncellenen sözlükler ve özelleştirilmiş sözlüklerle karşılaştırılarak taranır.
- **Yapılandırılmış veri aramaları,** mesajda özel bir yapılarda sunulan bilgiler bulunduğunda bu verilerin olası gizli veri olarak ele alınmasını sağlayarak, karmaşık dizilerde saklanan müşteri veritabanları hassas verilerin kontrol edilmesine imkan tanır.

ESNEK YÖNETİM
- **Yönetim kolaylığı,** tüm sunucu ortamının tek bir konsoldan merkezi olarak yönetilmesini sağlar. Sezgisel arabirim tüm sık kullanılan yönetim senaryolarını içerir.
- **Kolay anlaşılır bir yerleşime sahip tek pano**, tüm korunan sunucularda geçerli ürün durumu, veritabanı sürümü ve lisans durumuna eşzamanlı erişim sağlar.
- **Değiştirilen dosyaların yedeklenmesi**, bir kaza durumunda gerektiğinde orijinal dosyanın geri yüklenmesini sağlar ve değiştirilen dosyalara ait ayrıntılı yedekleme bilgileri destek araştırmalarında kullanılabilir.
- **Active Directory®** entegrasyonu Active Directory kullanıcılarına kimlik doğrulama uygulanmasını sağlar.

Kaspersky Security for Collaboration, Kaspersky Total Security for Business'e dahildir ve bu çözüm ayrı bir Hedeflenmiş Çözüm olarak da satın alınabilir.

*Bu ürün satın alınırken, gizli veri kaybı veya sızıntı önleme seçeneği ayrı olarak satılır.

► KASPERSKY SECURITY FOR STORAGE

EMC, NetApp, Hitachi ve IBM® Depolamalar için Yüksek Performanslı Koruma.

ÖNE ÇIKAN NOKTALAR

GÜÇLÜ, GERÇEK ZAMANLI KÖTÜ AMAÇLI YAZILIMDAN KORUMA
Ağa bağlı depolama (NAS) çözümleri için "Her Zaman Açık" proaktif koruma. Kaspersky'nin güçlü kötü amaçlı yazılımdan koruma motoru başlatılan veya değiştirilen her dosyayı virüsler, solucanlar ve Truva atları dahil olmak üzere her türlü kötü amaçlı yazılım türü açısından tarar. Gelişmiş sezgisel analiz yeni ve bilinmeyen tehditleri bile tanımlar.

PERFORMANS OPTİMİZASYONU
Optimize edilmiş tarama teknolojisi ve esnek hariç tutma ayarları içeren yüksek performanslı tarama, maksimum koruma sağlarken sistem performansı üzerindeki etkiyi en düşük düzeye indirir.

GÜVENİLİR
Birlikte kusursuz biçimde çalışacak şekilde tasarlanmış ve oluşturulmuş birleşik bileşenler kullanan basit mimari sayesinde olağanüstü hata toleransı sağlanır. Sonuç olarak kapatmaya zorlandığında güvenilir ve sürekli koruma için otomatik olarak yeniden başlatılan kararlı ve sağlam bir çözüm sunulur.

YÖNETİLMESİ KOLAY
Sunucular yeniden başlatma gerektirmeden "kutudan çıkar çıkmaz" uzaktan yüklenerek korunur ve basit, sezgisel bir merkezi konsol olan Kaspersky Security Center'ın yanı sıra diğer Kaspersky güvenlik çözümleri aracılığıyla birlikte yönetilir.

ÖZELLİKLER

HER ZAMAN AÇIK, PROAKTİF GÜVENLİK
Tehdit zekası alanında dünya çapında uzman olan kişiler tarafından tasarlanan sektör lideri Kaspersky kötü amaçlı yazılımdan koruma tarama motoru, geliştirilmiş algılama için akıllı teknolojiler kullanarak büyümekte olan ve potansiyel tehditlere karşı proaktif koruma sağlar.

OTOMATİK GÜNCELLEMELER
Kötü amaçlı yazılımdan koruma veritabanları, tarama işleminde herhangi bir kesintiye neden olmadan otomatik olarak güncellenmesi sayesinde sürekli koruma sağlar ve yönetici iş yükünü azaltır.

HARİÇ TUTULAN İŞLEMLER VE GÜVENİLİR BÖLGELER
Tarama performansı, tanımlanmış dosya biçimleri ve veri yedekleme gibi işlemlerle birlikte taramadan hariç tutulabilen, oluşturulmuş "güvenilir bölgeler" kullanılarak ayarlanabilir.

OTOMATİK ÇALIŞTIRMA NESNESİ TARAMA
Daha yüksek sunucu koruması için kötü amaçlı yazılımların sistem başlatılırken çalıştırılmasını engellemek amacıyla otomatik çalıştırma dosyası ve işletim sistemi taramaları yapılabilir.

OPTİMİZE EDİLMİŞ PERFORMANS İÇİN ESNEK TARAMA
Tarama ve yapılandırma süresini kısaltır ve yük dengelemeye yardımcı olarak sunucu performansının optimize edilmesini sağlar. Yönetici, tarama etkinliğinin derinliğini, genişliğini ve zamanlamasını belirleyip kontrol edebilir ve taranacak dosya türlerini ve alanları belirleyebilir. İsteğe bağlı tarama, sunucu etkinliğinin düşük olduğu dönemler için zamanlanabilir.

HSM ve DAS ÇÖZÜMLERİNİ KORUR
Hiyerarşik Depolama Yönetimi (HSM) sistemlerinin etkili biçimde korunması için çevrimdışı tarama modlarını destekler. Doğrudan Bağlı Depolama (DAS) koruması ise düşük maliyetli depolama çözümlerinin kullanılmasını destekler.

TÜM ANA PROTOKOLLERİ DESTEKLER
Kaspersky Security for Storage, farklı depolama sistemleri tarafından kullanılan ana protokolleri destekler: CAVA agent, RPC ve ICAP.

SANAL SİSTEMLER VE TERMİNAL SUNUCU KORUMASI
Esnek güvenlik, Hyper-V ve VMware sanal ortamlarındaki sanal (konuk) işletim sistemlerine ve Microsoft® ve Citrix terminal altyapılarına yönelik koruma içerir.

YÖNETİM

MERKEZİ KURULUM VE YÖNETİM
Bildirimler, güncellemeler ve esnek raporlama dahil olmak üzere uzaktan kurulum, yapılandırma ve yönetim işlemleri sezgisel Kaspersky Security Center aracılığıyla gerçekleştirilir. Tercih edilirse komut satırı yönetimi özelliği de sunulmaktadır.

YÖNETİCİ AYRICALIKLARININ KONTROLÜ
Her bir sunucunun yöneticisine farklı ayrıcalık düzeylerinin atanabilmesi, belirli kurumsal BT güvenlik ilkeleriyle uyumluluk sağlar.

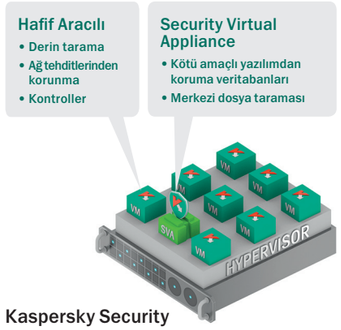
ESNEK RAPORLAMA
Raporlama, grafik raporlar olarak ya da Microsoft Windows® veya Kaspersky Security Center olay günlüklerinin incelenmesiyle sağlanabilir. Arama ve filtreleme araçları büyük hacimli günlüklere hızlı erişim olanağı sunar.

▶ KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization, ortamınıza hem koruma hem de performans sağlayan esnek bir çözümdür.

GELİŞMİŞ KORUMA İÇİN HAFİF ARACI

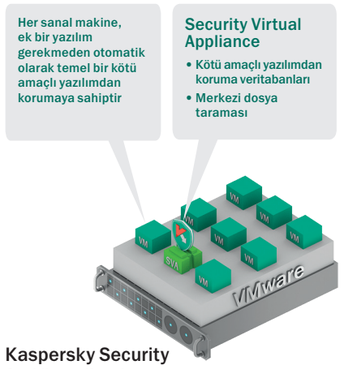
Kaspersky Security for Virtualization, her sanal makinede kurulu olan, güçlü ama hafif bir aracı içerir. Bu da gelişmiş uç nokta güvenlik özelliklerini etkinleştirmeye olanak tanır. Bu özellikler şunları içerir: Güvenlik açığı izleme; uygulama, cihaz ve web kontrolleri; anlık mesajlaşma, posta ve web için antivirüs koruması; gelişmiş sezgisel araçlar. Sonuç ise etkili performans ile birlikte güçlü, çok katmanlı güvenliktir.



Kaspersky Security for Virtualization
Hafif aracı yapılandırma

VMWARE ORTAMLARI İÇİN İSTEĞE BAĞLI ARACISIZ YAPILANDIRMA

VMware teknolojileriyle sıkı bir entegrasyon gerçekleştiğinde Kaspersky Security for Virtualization uygulaması kolayca kurulur ve bu platform üzerinden aracısız güvenlik yapılandırmasıyla yönetilir. Tüm güvenlik etkinlikleri Security Virtual Appliance üzerinde yoğunlaştırılmıştır. Security Virtual Appliance, sanal makinelerin otomatik olarak anında koruması için vShield ve ağ koruması için vCloud uygulamalarıyla birlikte çalışır.



Kaspersky Security for Virtualization
Aracısız yapılandırma*

TEMEL ÜRÜN ÖZELLİKLERİ

- **Kaspersky Security Center aracılığıyla merkezi yönetim**
- **Sanal makine korumasına dayalı merkezi SVA**
- **Gelişmiş kötü amaçlı yazılım koruması**
- **Ana bilgisayar tabanlı İzinsiz Giriş Önleme (HIPS) ve güvenlik duvarı**
- **Uygulamalar, web erişimi ve çevre birim cihazları için uç nokta kontrolleri**
- **Kaspersky Security Network aracılığıyla bulut yardımlı güvenlik**
- **Ağ Saldırısı Engelleyici**
- **Kimlik avı koruması**
- **Anlık mesaj, posta ve internet trafiği için anti-virüs**
- **Yeni sanal makineler için ek kurulum ve yeniden başlatma gerektirmez****

ESNEK LİSANSLANDIRMA

Kaspersky Security for Virtualization, ihtiyaçlarınıza bağlı olarak aşağıdaki lisans seçeneklerine sahiptir:

- Makine tabanlı lisanslandırma:
  - Masaüstü başına
  - Sunucu başına
- Kaynak tabanlı lisanslandırma:
  - Çekirdek başına.

ÇOKLU PLATFORMLAR: TEK MALİYET

Sadece bir Kaspersky Security for Virtualization lisansı Citrix, Microsoft® ve VMware tabanlı sanal ortamlar için destek içerir.

SECURITY VIRTUAL APPLIANCE (SVA)

Kaspersky Lab, bu alanda Security Virtual Appliance uygulamasına dayanan iki etkili çözüm sunar.

Kaspersky Lab'ın Security Virtual Appliance (SVA) uygulaması ana bilgisayar ortamındaki tüm sanal makineleri merkezi bir şekilde tarar. Bu mimari, AV taraması ile güncelleme "fırtınaları" ve "anlık" güvenlik açıklıklarını ortadan kaldırarak ve daha yüksek bir birleştirme oranı oluşturarak uç nokta kaynaklarından ödün vermeden etkili bir sanal makine koruması sağlar.

PLATFORM ARCHITECTURE İLE ENTEGRASYON

Kaspersky Security for Virtualization; VMware, Microsoft® Hyper-V® ve Citrix Xen platformlarını ve bu platformların çekirdek teknolojilerini destekler.

VMWare	Microsoft Hyper-V	Citrix Xen
High availability	Dynamic memory	Dynamic memory control
vCenter integration	Cluster shared volumes	Virtual machine protection and recovery (VMPR)
vMotion – ana makine DRS	Live backup	XenMotion (live migration)
Horizon view (tam klonlar ve bağlantılı klonlar)	Live migration	Multi-stream ICA
		Citrix receiver
		Personal vdisk

* Dosyaların karantina altına alınması, HIPS, güvenlik açığı taraması ve uç nokta kontrolleri gibi gelişmiş güvenlik özellikleri bu yapılandırmada mevcut değildir.

** Kalıcı olmayan sanal makinelerde ise hafif aracı sanal makinenin görüntüsüne dahil edildikten sonra anında koruma sağlanır. Kalıcı sanal makinelerde yönetici hafif aracı özelliğini yükleme sırasında manuel olarak kurmalıdır.

► KASPERSKY GÜVENLIK İSTİHBARAT HİZMETLERİ

CISO/kıdemli düzeyde güvenlik profesyoneli olarak kuruluşunuzu bugünün tehditlerine karşı korumak ve önümüzdeki yıllarda karşılaşılabilecek tehditleri öngörmek sizin sorumluluğunuzdadır. Bunun için çok az sayıda şirketin kendi kaynaklarını kullanarak oluşturabileceği bir stratejik güvenlik istihbaratına erişim gerekir.

Anlık istihbaratını farklı kanallarla paylaşmaya her zaman hazır olan, SOC/BT güvenlik ekibinizin kuruluşunuzu tüm çevrimiçi tehditlerden korumak için tam donanımlı olmasına katkı sağlayan Kaspersky Lab değerli bir iş ortağıdır.

SİBER GÜVENLİK EĞİTİMİ
Kaspersky Lab'ın Siber Güvenlik Eğitimi programı, altyapısını ve fikri mülkiyetini daha iyi korumak için siber güvenliğin rolünü öne çıkarmak isteyen tüm kuruluşları için özel olarak geliştirilmiştir.

Temel güvenlik süreçlerinden gelişmiş dijital adli deliler ve kötü amaçlı yazılım analizlerine kadar tüm öğelere kapsayan program, müşterilerin üç temel alanda siber güvenlik bilgilerini geliştirmesini sağlar:

- Temel konu başlığı bilgisi
- Dijital Adli Deliller ve Olaya Müdahale
- Kötü Amaçlı Yazılımdan Koruma ve Ters Mühendislik

TEHDİT VERİ MESAJLARI
Kaspersky Lab'ın Tehdit Veri Mesajları, mevcut Güvenlik Bilgileri ve Olay Yönetimi (SIEM) sistemlerinde veri istihbaratına anında entegrasyon sağlamak üzere tasarlanmıştır ve ek bir koruma katmanı sunar.

KÖTÜ AMAÇLI YAZILIM ANALİZİ; DİJİTAL ADLİ DELİLLER; OLAYA MÜDAHALE
Kaspersky Lab'ın Araştırma Hizmetleri, derinlemesine tehdit analizi sunarak ve olay çözümüne yönelik uygun adımlar konusunda danışmanlık sağlayarak kuruluşların savunma stratejilerini oluşturmalarına yardımcı olabilir.

Üç araştırma seviyesi sunulur:

- Kötü Amaçlı Yazılımdan Analizi, kuruluşunuzu hedef alan özel kötü amaçlı yazılım dosyalarının davranışlarını ve hedeflerini anlamanıza yardımcı olur.
- Dijital Adli Deliller, olayın eksiksiz bir resmini ve kuruluşunuzun nasıl etkilendiğini ortaya çıkarır.
- Olaya Müdahale, Kaspersky Lab uzmanlarının tesisi ziyaretini içeren tam olay araştırma döngüsüdür.

BOTNET TEHDİT İZLEME
Kaspersky Lab'ın uzman çözümü botnet'lerin etkinliğini izler ve kullanıcının bireysel çevrimiçi ödeme ve bankacılık sistemleriyle ilişkili tehditleri hızlı bir şekilde (20 dakika içinde) bildirir. Bu bilgileri müşterilerinizi, güvenlik hizmeti sağlayıcıları ve yasal mercileri güncel tehditler hakkında bilgilendirmek ve danışmanlık sağlamak için kullanabilirsiniz.

İSTİHBARAT RAPORLARI
Kaspersky Lab'ın İstihbarat Raporları 200 ülkede 80 milyondan fazla kullanıcının istatistiklerine dayalı ilgi çekici bilgilere anında erişebilmenize olanak sağlar. Bu raporlar, kuruluşunuzun karşı karşıya kaldığı tehditler hakkındaki farkındalığınızı ve bilgi düzeyinizi artırır.

Kaspersky Lab'ın bilgisi, deneyimi ve derin istihbaratı, dünyanın önde gelen emniyet güçleri ve devlet mercileri tarafından güvenilir bir ortak olarak kabul edilmesini sağlamıştır. Bu istihbaratı kuruluşunuz için bugün kullanabilirsiniz.

► KASPERSKY KURUMSAL ÇÖZÜMLER

DDOS KORUMASI — TAM SAVUNMA VE AZALTMA

İşletmenizi Dağıtılmış Hizmet Reddi saldırılarına karşı korumak için tüm gerekli adımları sağlar.

Kaspersky DDoS Koruması, işletmenizin tüm DDoS saldırısı türlerine karşı korunması ve etkilerin azaltılması için ihtiyaç duyulan her şeyi sunar. Bu yaklaşım, tüm çevrimiçi trafiğinizin sürekli analizini, olası saldırı varlığının bildirilmesini ve ardından yeniden yönlendirilen trafiğinizin alınmasını, trafiğinizin temizlenmesini ve "temiz" trafik durumuna geri dönülmesini kapsar.

BANKACILIK VE FİNANS KURULUŞLARI İÇİN KASPERSKY FRAUD PREVENTION

Çevrimiçi ve mobil finansal işlemler için dolandırıcılık risklerini ortadan kaldıran kapsamlı, özel tasarımlı ve kullanımı kolay teknoloji platformu.

Kaspersky Fraud Prevention, finans kuruluş müşterilerini söz konusu servislere erişmek için PC, dizüstü bilgisayar, akıllı telefon veya tablet kullanmalarından bağımsız olarak korur. Platform ayrıca banka tarafında kötü amaçlı yazılımı algılayan ve bireysel müşteri işlemlerindeki anormal davranış şablonlarını otomatik olarak belirleyen bir yazılım bileşeni içerir. Kaspersky Fraud Prevention for Endpoints yüklenmemiş olsa bile, İstemcisiz Motor dolandırıcılık amaçlı işlemlere karşı koruma sağlar.

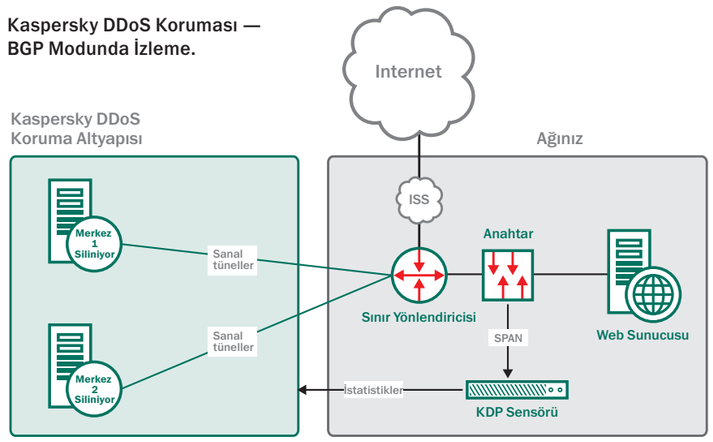
KRİTİK ALTYAPI KORUMASI

Sektörel kontrol sistemlerinin ve ağların güvenliğini sağlar

Kaspersky Endpoint Security for Business, ICS/SCADA uç noktalarını kritik sistemleri hedefleyen birçok suçlu için arka kapı seçeneği oluşturan tehditler ve güvenlik açıklarına karşı koruyan verimli bir "sektörel mod" koruması sağlar.

Emerson, Rockwell Automation ve Siemens gibi dünyanın lider otomasyon tedarikçileriyle birlikte çalışan Kaspersky Lab, müşteri tarafından yönetilen teknolojinin onay ve uyumluluk aşamalarına yönelik birçok özel prosedür geliştirmiştir. Bu yaklaşım, önemli altyapıları operasyon sürekliliğini ve tutarlılığını etkilemeden verimli şekilde korumamızı garanti altına alır.

Kaspersky DDoS Koruması — BGP Modunda İzleme.



KASPERSKY LAB PROFESSIONAL SERVICES

Karmaşık BT kurulumlarına sahip müşteriler için tasarlanan Kaspersky Profesyonel Uygulama ve Yükseltme, Eğitim ve Sağlık Kontrolü hizmetleri, Kaspersky Security for Business çözümlerinin doğru şekilde yapılandırılmasını, uygulanmasını ve optimum performans sunacak şekilde yönetilmesini sağlar.

KASPERSKY SMALL OFFICE SECURITY

Dünya Kalitesinde Güvenlik Küçük İşletmelerle Uyumlu Hale Getirildi.

Size özel zorluklar için size özel bir çözüm. Her zamankinden daha hızlı ve kullanımı kolay, dünya kalitesinde güçlü koruma.

- En fazla 25 kullanıcıya sahip işletmeler için özel olarak tasarlandı.
- Eğitim gerektirmeyen kolay kurulum ve kullanım.
- Her yerden internet tabanlı yönetim için web konsolu.

DENEYİM GEREKMEZ
Kaspersky Small Office Security, teknik konuda yeterli bilgiye sahip olmayan kişilerin kolayca yükleyebileceği ve çalıştırabileceği şekilde tasarlanmıştır. Basit kademelerden oluşan "sihirbazlarla" gelen paket, şu adımları gerçekleştirirken size otomatik olara yönlendirir:

- Tüm mevcut kötü amaçlı yazılımdan koruma yazılımlarının kaldırılması dahil kurulum
- Kontrolleri ayarlama, siz ve işletmeniz için en iyi sonucu ortaya çıkaran ilkeleri seçme
- Bu değişiklikleri birden fazla bilgisayara otomatik olarak tek seferde indirme

Her şeyin web tabanlı bir gösterge panosuyla yönetilmesi sayesinde, BT güvenliğiniz siz veya seçtiğiniz bir kişi tarafından internet üzerinden uzaktan yönetebilir.

Kaspersky Small Office Security, mükemmel güvenlik sunarken arka planda sorunsuz ve verimli şekilde çalışarak sizi koruyan bir uygulamanın varlığını unutmanızı sağlar.

ÇOK KATMANLI KORUMA
Kaspersky Small Office Security, PC ve Mac'leriniz, sunucularınız, tabletleriniz ve akıllı telefonlarınız için katmanlı koruma sağlar. Büyüyen işletmenizin ihtiyaç duyduğu tüm güvenlik araçları ve daha fazlası eksiksiz sağlanır. Kaspersky Small Office Security'nin BT güvenliğini üstleneceğinden ve sizin sadece işletmenizle ilgilenmenizi sağlayacağından emin olabilirsiniz.

- Yeni ve büyümekte olan siber tehditlere karşı bulut destekli, gerçek zamanlı koruma.
- Windows® ve Mac bilgisayarları, Windows sunucuları ve Android™ mobil cihazları korur.
- Ödüllü "Güvenli Para" teknolojisi çevrimiçi finans işlemlerini çevrimiçi korsanlar ve kimlik hırsızlarına karşı korur.
- Çalışanlarınızın web gezinmesini ve sosyal ağlarını yönetmenize olanak sağlayan kontroller.
- Gizli işletme ve müşteri verilerini koruyan şifreleme.
- Sahte ve kötü amaçlı web sitelerine karşı koruma sağlayan kimlik avı koruma teknolojileri.
- Güçlü spam filtreleme.
- Güvenli parola yönetimi.*
- Veri kaybını önlemek için Dropbox ile otomatik veri yedekleme.

PARANIZI KORUMANIZA YARDIMCI OLUR
Kaspersky Small Office Security, paranızı çalmayı hedefleyen korsan saldırılarına karşı koruma sağlamanın yanı sıra çalışanların erişimini düzenlemenize ve internette gezinme veya mesajlaşma kontrolleri ayarlamanıza imkan tanıyarak çalışanlarınızın daha verimli olmasını sağlar. Şifreleme gibi gelişmiş güvenlik özellikleri müşteri verilerini güvenle saklamanıza olanak sağlayarak, satış potansiyelinize ve müşteri memnuniyetine katkı sağlar.

* Sadece 32 bit uygulamalarla kullanılabilir. Android ve iOS cihazlarını içerir.

KASPERSKY BAKIM VE DESTEK SÖZLEŞMELERİ

İç rahatlığı ve optimum çalışma süresi arayan kuruluşlar için olaylar, yapılandırma sorunları, uyumsuzluk durumları ve diğer BT güvenlik karmaşıklıklarına yönelik destek.

Kaspersky Lab'ın Bakım ve Destek Sözleşmeleri (MSA'lar) kuruluşunuzun BT güvenlik ağları için çalışma süresi garantisi ve sürekli kalite bakımı sunar. Bu sözleşmeler, yanlış yapılandırmadan kötü amaçlı yazılım saldırılarına kadar beklenmeyen olaylarda üstün destek sağlayarak, kuruluşunuzun tüm faaliyetlerini dengeli ve verimli şekilde yürütmesine katkıda bulunur.

Kaspersky Lab Bakım ve Destek Sözleşmeleri aşağıdaki sorunlara yönelik çözümleri kapsar:

- Beklenmeyen küresel virüs saldırıları
- Karmaşık altyapıdan kaynaklanan uzun kapalı kalma süreleri
- Uygulama optimizasyonu ve özelleştirilmiş yamalar
- Ağ uyumsuzluk sorunları
- Kaspersky Lab ürün yükseltme işlemi
- Kötü amaçlı yazılım olayı araştırması
- Ürün kurulumu ve yapılandırma desteği*
- Yama ve diğer güncelleme uygulamaları*

Ekibinizin ne zaman yardıma ihtiyacı olsa Kaspersky Lab uzmanları yerel dillerde sunulan özel öncelikli hatlarla ve kuruluşunuzun gereksinimlerine göre tasarlanan pencerelerle her zaman yanınızdadır. Aşağıdaki matris mevcut destek seçeneklerini açıklar.

	Standart Destek		Genişletilmiş Destek	
	MSA Starter	MSA Plus	MSA Business	MSA Enterprise
Ayrıcalıklı Telefon Hattı	Evet	Evet	Evet	Evet
Teknik Hesap Yöneticisi	Hayır	Hayır	Evet	Evet, Özel
Yerel Dil Desteği	8x5	8x5	8x5	24x7x365
Önem Düzeyi 1 Destek	8x5	8x5	24x7x365	24x7x365
Önem Düzeyi 1 Yanıt Süresi	8 İş Saati	6 İş Saati	4 Saat	30 Dakika
Önem Düzeyi 2 Destek	8x5	8x5	8x5	24x7x365
Profesyonel Hizmet Danışmanlık	Hayır	Hayır	Ek Maliyet	Sağlık Kontrolü ve Özel Raporlama
Olay Sınırlama	6	12	36	Sınırlı

* Ödemeli MSA Business seçenekleri MSA Starter ve MSA Plus Kullanılamaz.

KASPERSKY LAB WORLDWIDE

Kaspersky ofisleri, dünyanın dört bir tarafındaki yerel ve küresel boyuttaki işletmeleri destekler. Kaspersky Security for Business çözümlerini nasıl alabileceğiniz hakkında daha fazla bilgi için lütfen yerel bayinizle iletişime geçin.

www.kaspersky.com

Asya Pasifik

1. Avustralya
2. Çin
3. Hong Kong
4. Hindistan
5. Kore
6. Malezya

Avrupa

7. Avusturya
8. Fransa
9. Almanya
10. İtalya
11. Hollanda
12. Portekiz
13. İspanya
14. Norveç
15. İsviçre
16. Birleşik Krallık

Yükselen Piyasalar

17. Letonya
18. Polonya
19. Romanya
20. Slovenya
21. Güney Afrika
22. Türkiye
23. Ukrayna
24. Birleşik Arap Emirlikleri

Japonya

25. Japonya (Tokyo)

Kuzey Amerika

26. Kanada
27. ABD (Boston)
28. ABD (Miami)

Rusya ve CIS

29. Rusya
30. Kazakistan


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab, Moskova, Rusya
www.kaspersky.com

İnternet güvenliği ile ilgili her şey için:www.securelist.com

Size yakın bir ortak bulun:
www.kaspersky.com/buyoffline

Catalog_SP1/Feb15/Global

KASPERSKY lab