KASPERSKY KURUMSAL ÜRÜNLER 2013

Gör. Denetle. Koru.

KASPERSKY lab

KASPERSKY LAB HAKKINDA

Kaspersky Lab dünyanın en büyük bağımsız güvenlik yazılımı şirketidir. Kötü amaçlı yazılımlara karşı güçlü koruma, esnek denetim araçları, kriptolama teknolojisi ve sistem yönetim araçlarının bir bileşimiyle kuruluşunuz için mümkün olan en iyi BT güvenliğini sağlıyoruz. Kaspersky güvenliği; uç noktadan sunucularınıza ve ağ geçitlerine kadar uzanır ve benzersiz bütünleşmiş tasarım yaklaşımı altyapınızın boyutu ne olursa olsun fiziksel, sanal ve mobil cihazlarınızı tek bir merkezi yönetim konsolundan güvence altına alıp denetleyebileceğiniz anlamına gelir. Kaspersky teknolojisi, dünya genelinde, sektörün önde gelen BT üreticilerinin ve yayıncılarının ürünlerinde ve hizmetlerinde de kullanılır.

Daha fazla bilgi için: www.kaspersky.com.tr

En son anti-virüs, casus yazılımdan koruma, istenmeyen postadan korunma ve diğer IT güvenliği konuları ve eğilimleri için şu adresi ziyaret edin: www.securelist.com.

SEKTÖRÜN GERÇEKTEN BÜTÜNLEŞMİŞ TEK GÜVENLİK PLATFORMU

TEK KONSOL
Kaspersky ürünleri yöneticinin tüm güvenlik alanını, sanal makineleri, fiziksel ve mobil cihazları ‘tek bir yerden’ görüntüleyebileceğiniz ve yönetebileceğiniz şekilde tasarlanmıştır.

TEK PLATFORM
Biz Kaspersky Lab olarak diğer şirketlerden teknoloji satın almak yerine kendi konsolumuzu, güvenlik modüllerimizi ve araçlarımızı kurum içinde geliştiriyoruz. Aynı kod tabanında çalışan aynı programcılar birlikte konuşan ve çalışan teknolojileri geliştiriyor. Sonuç istikrar, bütünleşmiş ilkeler, yararlı raporlama ve sezgisel araçlardır.

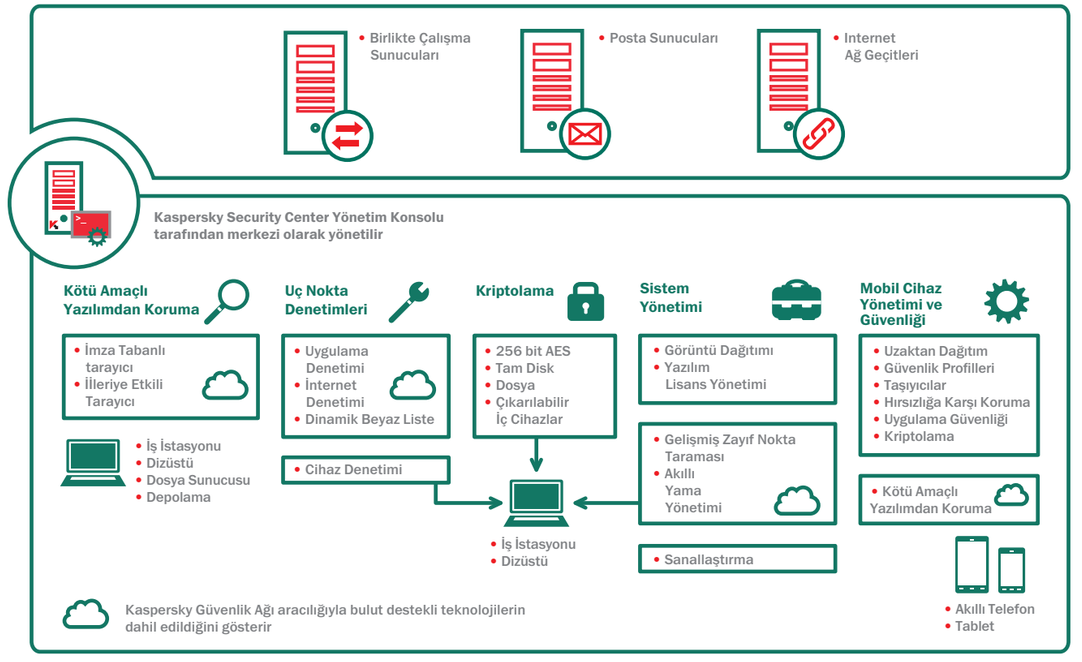
TEK MALİYET
Tüm Kaspersky ürünleri ve araçları tek bir üreticiden gelir ve tek bir kurulum içinde teslim edilir. Bu nedenle güvenlik risklerinizi iş hedeflerinize uygun hale getirmeyi, her istediğinizde yeni bir bütçeleme ve gerekçelendirme sürecinden geçmeniz gerekmez.

SİZİN İÇİN DOĞRU ÇÖZÜM

Kaspersky Security for Business; aradığınız ister (işistasyonlarından akıllı telefonlara ve sanal makinelere kadar) uç noktalarınızı korumak ve denetlemek, ister sunucularınızı veya ağ geçitlerinizi güvence altına almak, isterse de tüm güvenlik ortamınızı uzaktan yönetmek olsun, kuruluşunuz için en doğru çözümü sunar.

Kaspersky kriptolama ve mobil cihaz yönetiminden yama yönetimine ve lisans bilgilerine kadar kapsamlı bir teknoloji listesine sahip olmakla övünüyor. Müşterilerimizin giderek daha karmaşıklaşan ve çeşitlenen siber tehditlerle mücadele etmek için gerek duydukları dünya çapında korumayı vermek için, hepsi bulut tabanlı Kaspersky Güvenlik Ağının desteğine sahip olarak sorunsuz bir şekilde birlikte çalışır.

Kısacası, BT dünyanızı görmenizi, denetlemenizi ve korumanızı kolaylaştıran, sektörün temelden itibaren kurulmuş ilk Güvenlik Platformunu veriyoruz.

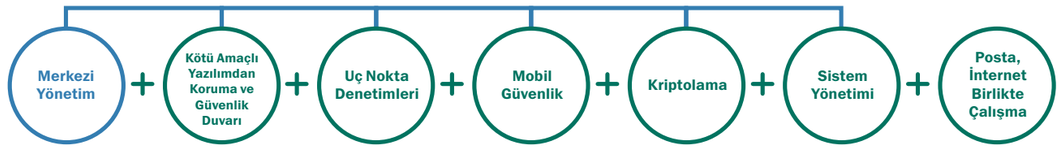


KASPERSKY SECURITY FOR BUSINESS

Teknolojilerimiz ve sizin için nasıl birlikte çalıştıkları

	Core	Select	Advanced	Total	Managed by Security Center	Available in a Targeted Solution
Kötü Amaçlı Yazılımdan Koruma	•	•	•	•	•	
Güvenlik Duvarı	•	•	•	•	•	
Uygulama Denetimi		•	•	•	•	
Cihaz Denetimi		•	•	•	•	
İnternet Denetimi		•	•	•	•	
Dosya Sunucuları		•	•	•	•	•
Mobil Uç Nokta Koruması		•	•	•	•	•
Mobil Cihaz Yönetimi		•	•	•	•	•
Kriptolama Teknolojisi			•	•	•	
OS Görüntü Yönetimi			•	•	•	•
Lisans Yönetimi			•	•	•	•
Zayıf Nokta Yönetimi			•	•	•	•
Yama Yönetimi			•	•	•	•
Ağ Giriş Denetimi			•	•	•	•
Birlikte Çalışma				•		•
Posta Sunucuları				•		•
İnternet Ağ Geçitleri				•		•
Sanallaştırma					•	•
Depolama					•	•

KASPERSKY ENDPOINT SECURITY FOR BUSINESS



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 Yönetimi**nden (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:

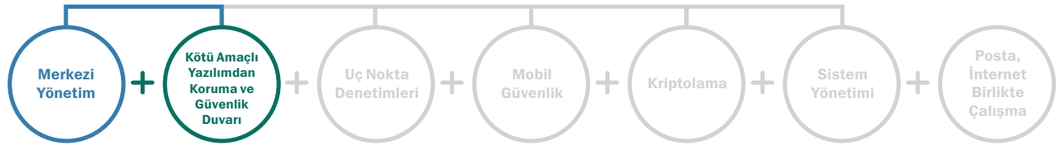
- Görüntü Yönetimi modülünü kullanarak görüntü oluşturma ve sistemlere dağıtma.
- Gelişmiş Zayıf Nokta Taraması ve Akıllı Yama Yönetiminin güçlü bileşimiyle donanım ve yazılımların zayıf noktalarını düzeltmeye öncelik verme.
- Yazılım Lisans Yönetimiyle lisans kullanımını ve uygunluğunu izleme.
- Ağ 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.

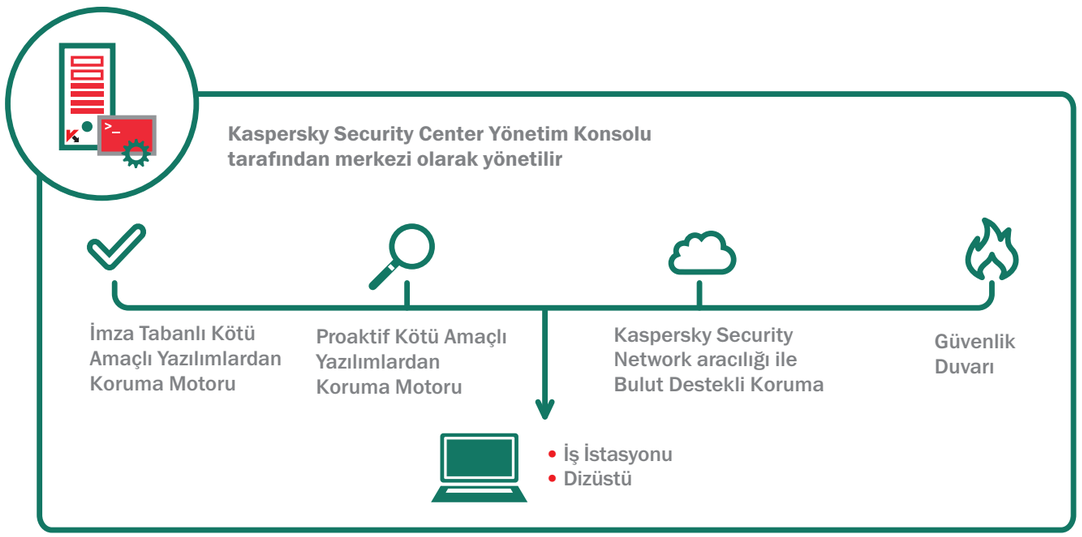
KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Core



Merkezi dağıtım, yönetim ve raporlamayla birlikte ödüllü kötü amaçlı yazılımdan koruma.

Katmanlı bir güvenlik modeli kötü amaçlı yazılımdan korumanın en iyisiyle başlar. Kaspersky kötü amaçlı yazılımları tespit etmenin ve kaldırmanın lideri olarak bilindiğine göre bundan daha iyi bir temel olamaz. Kaspersky Endpoint Security for Business 'CORE' katmanı Kaspersky Security Center tarafından merkezi olarak yöneltir ve bulut tabanlı Kaspersky Güvenlik Ağıyla desteklenir.



Kaspersky Endpoint Security for Business CORE Katmanı — Bulut Destekli Koruma özelliğiyle kötü amaçlı yazılımlardan güçlü korunma.

TEMEL ÖZELLİKLER:

UÇ NOKTA KÖTÜ AMAÇLI YAZILIMLARINDAN GÜÇLÜ KORUNMA
Kaspersky'nin tarama motorları, işletim sisteminde birden fazla düzeyde çalışarak kötü amaçlı yazılımları yok eder.

BULUT ETKİN KORUMA
Kullanıcılar yeni tehditlere karşı bulut tabanlı Kaspersky Güvenlik Ağıyla gerçek zamanlı olarak korunur.

MERKEZİ YÖNETİM
Yöneticiler, aynı konsoldan, mevcut anti-virüs yazılımını merkezi olarak kaldırabilir, Kaspersky'i yapılandırıp dağıtabilir ve raporlamayı gerçekleştirebilir.

UÇ NOKTA KÖTÜ AMAÇLI YAZILIMDAN KORUNMA ÖZELLİKLERİ:

SIK GÜNCELLEMELER VE İMZA TABANLI KORUMA
Kötü amaçlı yazılım tehditlerini tespit etmek için, sektörde kendini kanıtlamış geleneksel imza tabanlı yöntem.

SİSTEM İZLEYİCİSİ TARAFINDAN GERÇEKLEŞTİRİLEN DAVRANIŞ ANALİZİ
Kaspersky Güvenlik Ağı (KSN) tehdit şüphelerine geleneksel koruma yöntemlerinden çok daha hızlı yanıt verilmesini sağlar. KSN'in yanıt süresi 0,02 saniye kadar kısa olabilir!

KİŞİSEL GÜVENLİK DUVARIYLA ANA MAKİNE TABANLI SIZMA ÖNLEME SİSTEMİ (HIPS)
En yaygın uygulamaların yüzlercesi için ön tanımlı kurallar güvenlik duvarının yapılandırılmasına ayrılan süreyi kısaltır.

GENİŞ PLATFORM DESTEĞİ
Kaspersky, çeşitli ağları destekleyerek yöneticinin iş yükünü kolaylaştırarak Windows®, Macintosh® ve Linux® için uç nokta güvenliği sunar.

KASPERSKY SECURITY CENTER'IN ÖZELLİKLERİ:

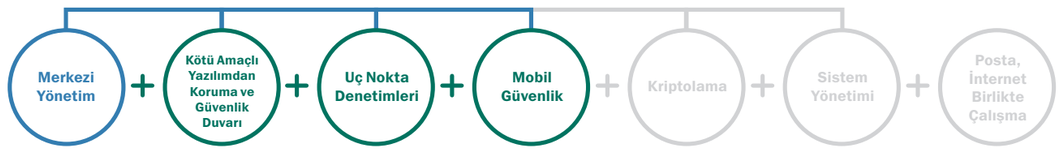
TEK MERKEZİ KONSOL
Kaspersky koruma uç noktalarınızın tümü için uzaktan yönetim.

SEZGİSEL KULLANICI ARABİRİMİ
Karışık olmayan bir gösterge tablosundaki açık ve işleme konabilir bilgiler yöneticilerin gerçek zamanlı koruma durumunu görmesine, ilkeleri ayarlamasına, sistemleri yönetmesine ve raporları almasına olanak verir.

İNTERNET ARABİRİMİ
Koruma durumunu uzaktan izler ve esnek ve erişebilir bir arabirimle temel olayları rapor eder.

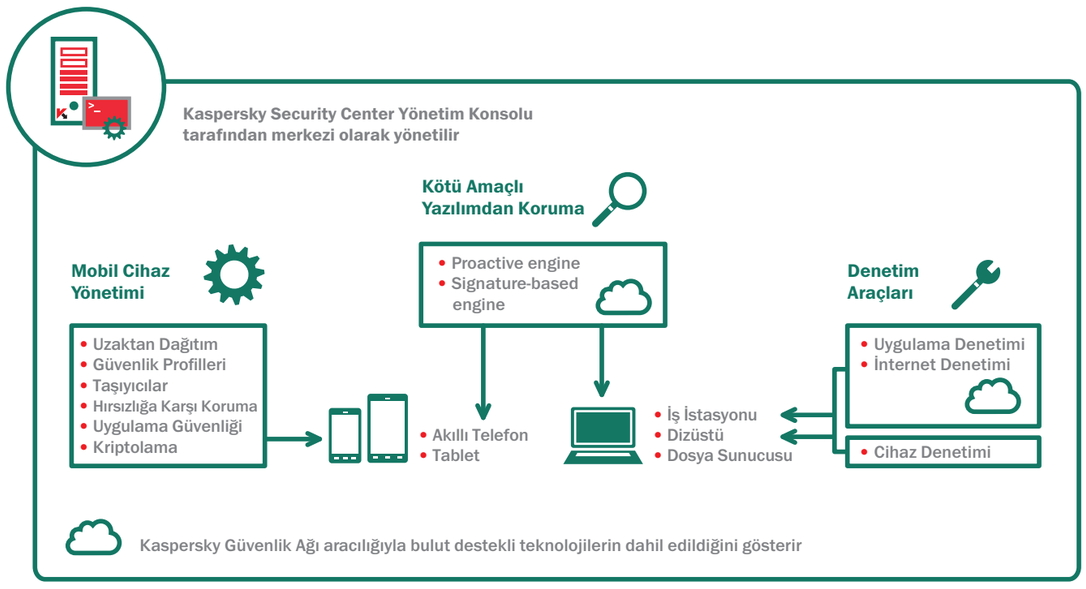
ÖLÇEKLENEBİLİR DESTEK
Kaspersky Security Center, altyapınızın büyüklüğü ne olursa olsun, büyüyen ihtiyaçlarınızı karşılamak için dağıtım ve yönetim araçları, esnek ilke seçenekleri ve dayanıklı raporlama sunar.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS
Select



Mobil iş gücünü etkinleştirme, BT güvenlik ilkesinin uygunluğunu sağlama ve kötü amaçlı yazılımları engelleme araçları.

Kaspersky'nin 'SELECT' katmanı mobil cihaz dağıtımını ve Mobil Cihaz Yönetimi (MDM) aracılığıyla korumayı ve mobil kötü amaçlı yazılımdan korumayı içerir. Uç nokta denetimleri (internet, cihaz ve uygulama) BT ortamınızın temel unsurlarını güvenli tutarak kuruluşunuzun BT ilkesini uygulamanıza yardım eder.



Kaspersky Endpoint Security for Business — SELECT Katmanı. Denetim araçları ve Mobil Güvenlik özellikleri.

TEMEL ÖZELLİKLER:

UÇ NOKTALARI KÖTÜ AMAÇLI YAZILIMA KARŞI GÜÇLÜ KORUMA
Kaspersky'nin 'türünün en iyisi' tarama motoru kötü amaçlı yazılımları yok etmek için işletim sisteminde birden fazla düzeyde çalışır. Bulut tabanlı Kaspersky Güvenlik Ağı (KSN) kullanıcıları yeni tehditlere karşı gerçek zamanlı korur.

ESNEK, GRANÜLER DENETİM ARAÇLARI
Güvenli olan ve olmayan uygulamaların ve internet sitelerinin sınıflandırılmış, bulut tabanlı bir veritabanı yöneticilerin uygulamalar ve internette gezinme için ilkeleri uygulamasına yardımcı olurken granüler denetimler yalnızca belirli cihazların ağdaki makinelere takılabilmesini sağlar.

AKILLI TELEFONLAR VE TABLETLER İÇİN ETKİLİ DAĞITIM VE GÜVENLİK
Android™, BlackBerry®, Symbian ve Windows® mobil cihazlar için aracı tabanlı mobil güvenlik mevcuttur. Mobil cihaz ilkeleri ve yazılımları bunlara ve iOS cihazlarına Kaspersky MDM aracılığıyla kablosuz olarak güvenli şekilde dağıtılabilir.

BU KATMANDA UYGULANANLAR:

UÇ NOKTA DENETİMLERİ:

UYGULAMA DENETİMİ
BT yöneticilerinin uygulamalara (veya uygulama kategorilerine) izin veren, engelleyen veya düzenleyen ilkeleri ayarlamasını sağlar.

CİHAZ DENETİMİ
Kullanıcıların veri ilkelerini, çıkarılabilir depolama ve USB veya başka bir veri yolu türüyle bağlı diğer çevre cihaz denetimleriyle birlikte, ayarlamasına, zamanlamasına ve uygulamasına olanak verir.

İNTERNET DENETİMİ
Uç nokta tabanlı gezinme denetimleri, kullanıcının kurumsal ağda veya dolaşırken izleneceği anlamına gelir.

DİNAMİK BEYAZ LİSTE
Kaspersky Güvenlik Ağı tarafından sağlanan gerçek zamanlı dosya saygınlıkları onaylanmış uygulamalarınızın kötü amaçlı yazılımlardan arınmış olmasını sağlar ve kullanıcının verimini azamileştirmeye yardımcı olur.

KASPERSKY SECURITY FOR MOBILE:

KÖTÜ AMAÇLI YAZILIMDAN KORUNMA TEKNOLOJİLERİ
İmza tabanlı, ileriye etkili ve bulut destekli bileşik tespitin sonucu gerçek zamanlı korumadır. Güvenli bir tarayıcı ve anti-spam, güvenliği arttırır.

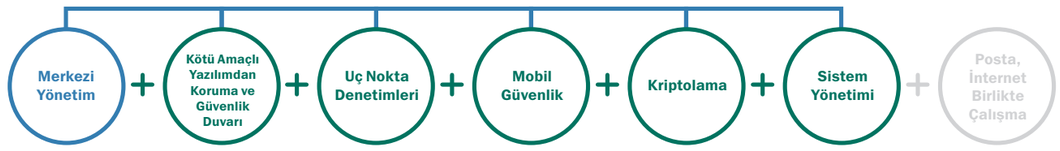
KABLOSUZ (OTA) YAPILANDIRMA
SMS, e-posta ve PC'yi kullanarak uygulamaları merkezi olarak ön yapılandırma ve dağıtma özelliği.

HIRSIZLIĞA KARŞI UZAK ARAÇLAR
SIM-Watch, Uzaktan Kilitle, Temizle ve Bul özelliklerinin tümü, bir mobil cihaz kaybolmuş veya çalınmışsa, kurumsal verilere izinsiz erişimi engeller.

MOBİL CİHAZLAR İÇİN UYGULAMA DENETİMİ
Mobil bir cihazda kurulu olan uygulamaları ön tanımlı grup ilkelerine göre izler. Bir "Zorunlu Uygulama" grubu içerir.

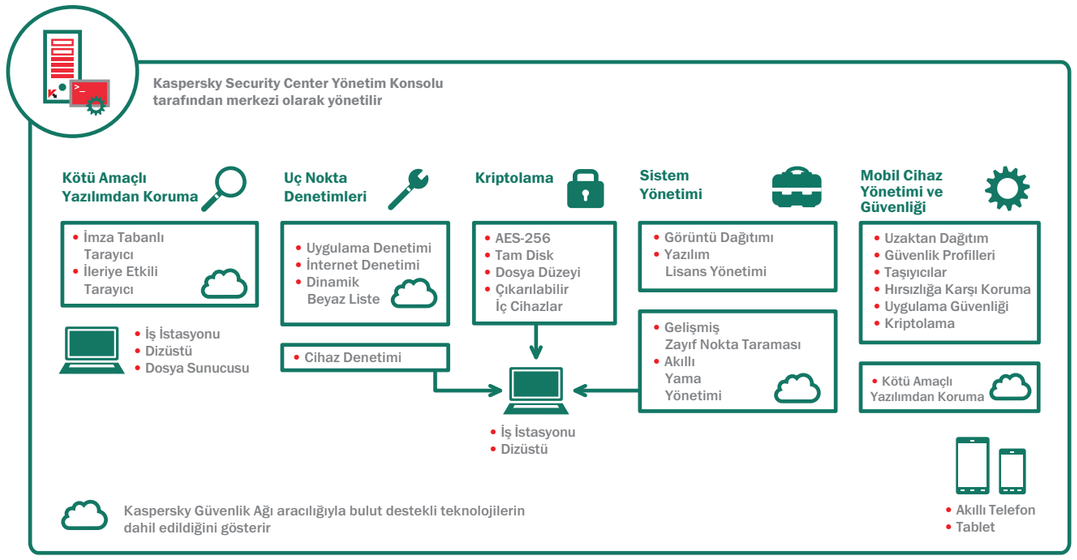
ÇALIŞANLARIN SAHİP OLDUĞU CİHAZLARA DESTEK
Kurumsal veriler ve uygulamalar, kullanıcıya açık olan, şifreli taşıyıcılarda yalıtılır. Bu veriler ayrıca temizlenebilir.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS
Advanced



Kaspersky Lab'ın bu değerli çözümler dizisinde bol bulunan BT optimizasyonu özellikleriyle birleştirilmiş güvenlik araçları.

Kaspersky'nin Advanced katmanı BT ilkesini uygulamak, kullanıcıları kötü amaçlı yazılımlardan korumak, veri kaybını engellemek ve BT verimliliğini arttırmak için koruma ve yönetim çözümleri sağlar.



Kaspersky Endpoint Security for Business — ADVANCED Katmanı. Kriptolama Teknolojisi ve Güvenlik Sistemleri Yönetimi özelliklerine sahiptir.

TEMEL ÖZELLİKLER:

GÜÇLÜ KRİPTOLAMA TEKNOLOJİSİ
Tam disk ve klasör düzeyinde AES 256 bit kriptolama kayıp veya çalınmış verileri korur ve tümü kullanıcıya açık olan verilerin çıkarılabilir cihazlar, e-posta, ağ veya web aracılığıyla güvenli paylaşımına imkan verir.

SİSTEM YAPILANDIRMASI VE YAMA YÖNETİMİ
Kullanıcı dostu merkezi bir konsoldan yönetilen tümüyle bütünleşmiş bir araç kitini sağlamak üzere işletim sistemi görüntüsünün oluşturulması ve dağıtılması, zayıf nokta taraması, otomatik yama yönetimi, Ağ Giriş Denetimi, envanterler ve lisans yönetimi birleştirir.

AKILLI TELEFONLAR VE TABLETLER İÇİN MOBİL DAĞITIM VE GÜVENLİK
Kaspersky MDM ile aracı tabanlı mobil uç nokta güvenliği ve uzak cihaz ve yazılım ilkesi yönetimi.

KÖTÜ AMAÇLI YAZILIMLARA KARŞI GÜÇLÜ UÇ NOKTA KORUMASI VE ESNEK DENETİMLER
Kaspersky'nin bulut destekli 'türünün en iyisi, kötü amaçlı yazılımdan korunma ve granüler uygulamalar, internet ve cihaz denetimi araçları.

BU KATMANDA UYGULANANLAR:

KRİPTOLAMA VE VERİ KORUMASI:

KAPSAMLI KRİPTOLAMA
Cihazın çalınması veya kaybolması durumunda kritik iş bilgilerinin güvence altına almak için, 256 bit kriptolamayla Advanced Encryption Standard (AES) tarafından desteklenen tam disk veya dosya düzeyini seçin.

GÜVENLİ VERİ PAYLAŞIMI
Verileri çıkarılabilir cihazlar, e-posta, ağ veya internet aracılığıyla paylaşırken korunmasını sağlamak için şifreli ve kendiliğinden açılan paketler oluşturun.

ÇIKARILABİLİR CİHAZLAR İÇİN DESTEK
İlkeler aracılığıyla veri kriptolamayı çıkarılabilir cihazlarda uygulayarak güvenliğinizi arttırır.

SON KULLANICILARA AÇIK
Kaspersky'nin kriptolama çözümü sorunsuzdur ve kullanıcılar tarafından görünmez ve verimlilik üzerinde hiçbir olumsuz etkisi yoktur. Uygulama ayarları ve güncellemeler üzerinde de hiçbir etkisi yoktur.

SİSTEM YAPILANDIRMASI VE YAMA YÖNETİMİ

YAMA YÖNETİMİ
Yamaların otomatik dağıtımıyla birleştirilen zayıf noktaların gelişmiş ayrıntılı taraması.

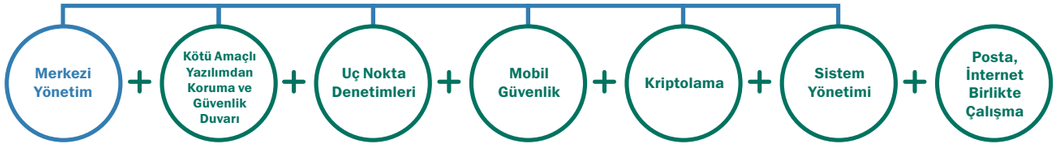
İŞLETİM SİSTEMİ VE UYGULAMA GÖRÜNTÜSÜNÜN DAĞITIMI
Merkezi bir yerden sistem görüntülerini kolay oluşturma, depolama ve dağıtma. Microsoft® Windows® 8'e taşımak için mükemmel.

YAZILIMLARIN UZAKTAN DAĞITIMI
Yazılımların, şube ofislerinde olsalar bile, istemci makinelere merkezi dağıtımı.

AĞ GİRİŞ DENETİMİ (NAC)
Ağ Giriş Denetimi (NAC) ile bir 'konuk' ilkesi oluşturabilirsiniz. Konuk cihazlar (mobil cihazlar dahil) otomatik olarak tanınır ve doğru kimlik parolasıyla, onayladığınız kaynakları kullanabilecekleri bir kurumsal portala gönderilirler.

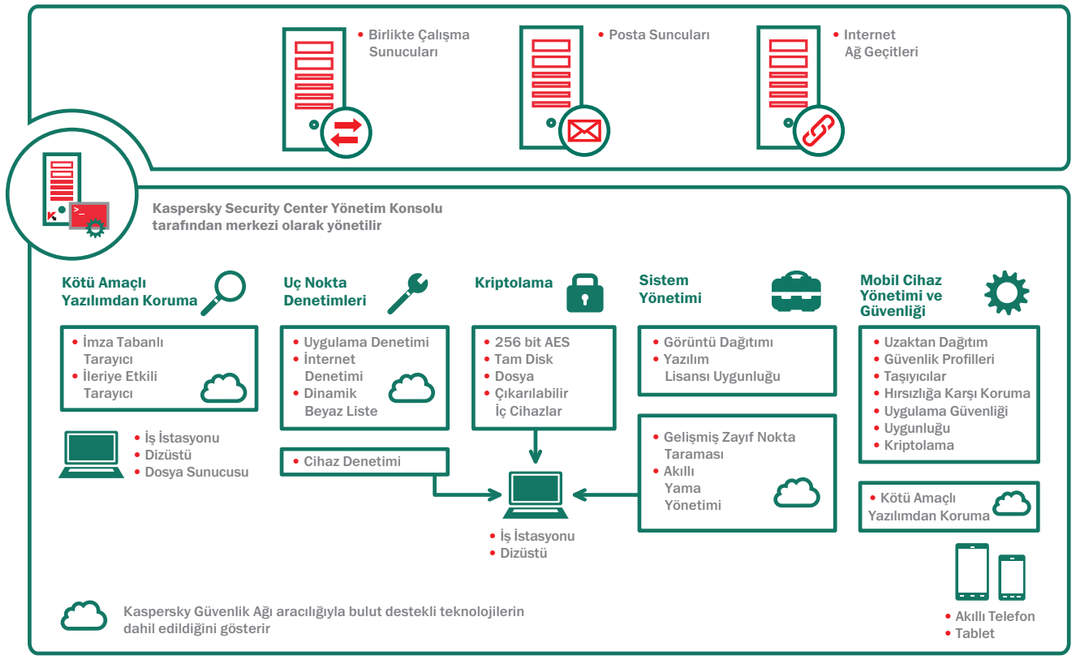
DONANIM, YAZILIM VE LİSANS DENETİMİ
Donanım ve yazılım bilgileri raporları yazılım lisansı yükümlülüklerini denetlemenizi sağlar. Böylece yazılım haklarını merkezi olarak tedarik ederek masrafları azaltabilirsiniz.

KASPERSKY TOTAL SECURITY FOR BUSINESS



Kötü amaçlı yazılımlara karşı uçtan uca koruma, kriptolama, kapsamlı BT verimliliği ve ilke uygulama araçları.

Kaspersky Total Security for Business bugün sektörde sunulan en eksiksiz koruma ve yönetim platformunu veriyor. Total Security for Business ağınızın her katmanını korur ve kullanıcılarınızın kullandıkları cihaz veya bulundukları yere bakılmaksızın, verimli olması ve kötü amaçlı yazılımlardan korunmasını sağlamak için güçlü yapılandırma araçları ekler.



TEMEL ÖZELLİKLER:

Önceki üç katmanın özelliklerine ek olarak:

POSTA SUNUCUSU KORUMASI
Tüm popüler posta sistemleri için posta trafiğini kötü amaçlı yazılıma karşı koruma ve istenmeyen posta koruması.

İNTERNET AĞ GEÇİTLERİ İÇİN GÜVENLİK
HTTP(S)/FTP/ SMTP ve POP3 trafiğindeki kötü amaçlı ve potansiyel olarak saldırgan programları otomatik olarak kaldırarak güvenli internet erişimini sağlayın.

BİRLİKTE ÇALIŞMA GÜVENLİĞİ
Kaspersky, içerik ve dosya filtreleme özellikleri uygunsuz içeriğin depolanmasına yardım ederken SharePoint® sunucularınızı kötü amaçlı yazılımlara karşı korur.

BU KATMANDA UYGULANANLAR:

POSTA SUNUCULARI:

POSTA TRAFİĞİNİ KORUMA
Büyük posta ve işbirliği platformlarının en son sürümlerindeki postaları koruma: Microsoft Exchange, IBM Lotus Domino ve Linux tabanlı posta sunucuları.

ANTI-SPAM İÇİN KSN BÜTÜNLEŞTİRMESİ
Kaspersky Lab'ın bulut tabanlı tehdit tespit motoru (KSN) ile bütünleşme sayesinde istenmeyen postaların tespit edilme oranını arttırır.

AZALTILMIŞ TRAFİK YÜKÜ
Bulut etkin, akıllı istenmeyen posta filtreleme trafik yükünü önemli ölçüde azaltır.

SİSTEM KAYNAĞI OPTİMİZASYONU
Yeni bir anti-virüs motoru, sunucu kaynaklarının yük dengelemesi ve tarama istisnalarının hepsi sisteminizdeki yükü azaltır.

İNTERNET AĞ GEÇİTLERİ:

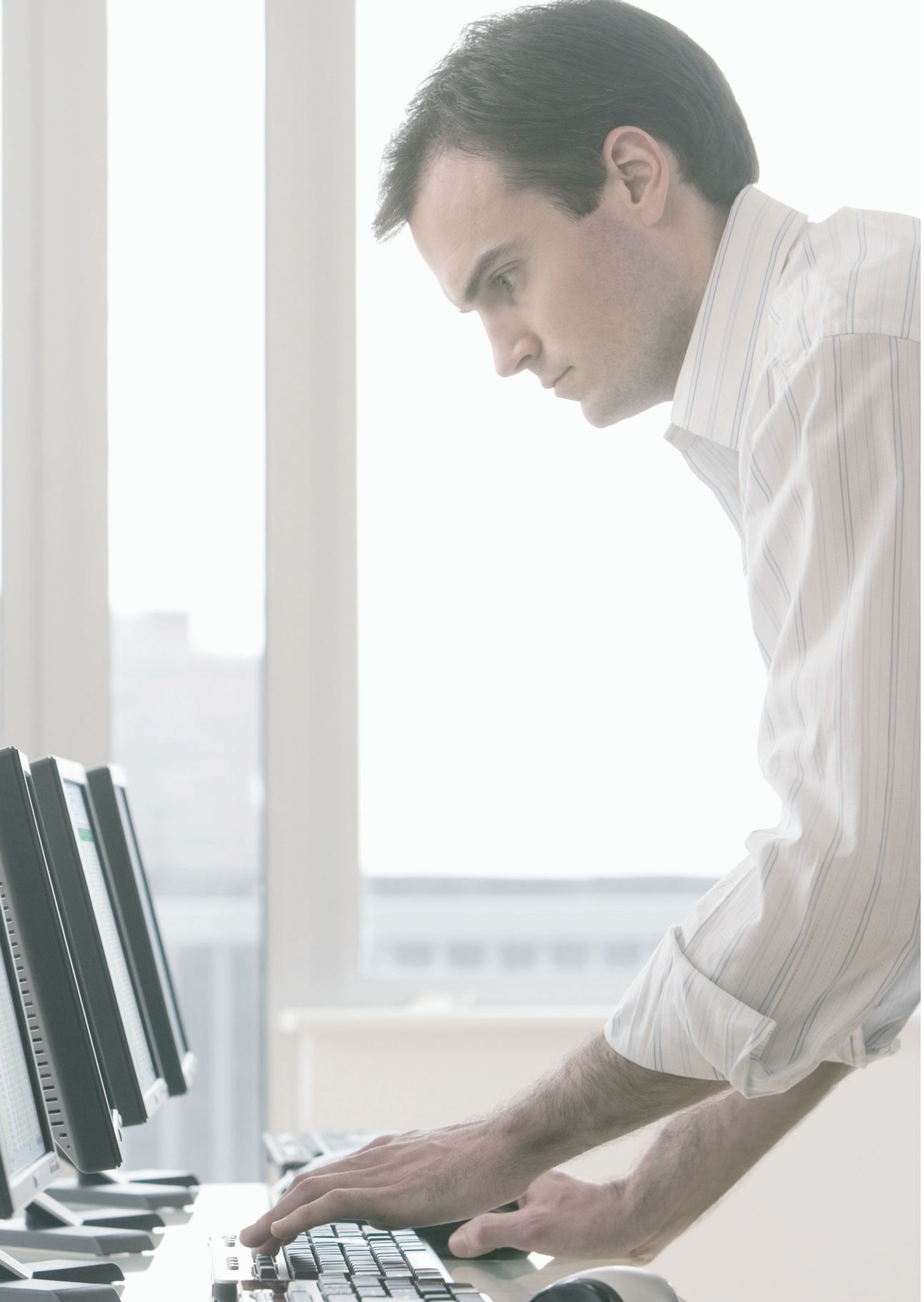
YÜKSEK PERFORMANS
Güçlü bir anti-virüs motoruna ek olarak optimize edilmiş, akıllı tarama teknolojisi ve yük dengeleme performansı arttırır ve virüs taraması için gereken kaynakları azaltır.

BİRDEN FAZLA PLATFORM DESTEĞİ
Kaspersky Security for Internet Gateway, Windows ve Linux platformlarına dayalı en popüler ağ geçitlerini destekler.

BİRLİKTE ÇALIŞMA

SHAREPOINT ÇİFTLİKLERİ İÇİN KÖTÜ AMAÇLI YAZILIM ENGELİ
Yükleme indirme denemelerinden kötü amaçlı yazılımları gerçek zamanlı olarak tespit edip engellemek üzere tasarlanmış yenilikçi tespit teknolojisini kullanır.

İÇERİK FİLTRELEME
Dosya türlerine veya metin içeriğine göre, uygunsuz dış yüklemelerin engellenmesine, iç iletişim ilkelerinin uygulanmasına ve uygunsuz dosyaların depolanmasının engellenmesine yardımcı olur.



KASPERSKY ANTI-VIRUS FOR STORAGE

Kaspersky Anti-Virus for Storage ağ depolama ürünlerinin EMC Celerra ailesini her türden kötü amaçlı yazılımdan korur.

Bir ağdaki veri depolama sistemleri her büyüklükte kuruluşların çalışanlarına bilgilere hızlı ve kolay paylaşılmış erişim sağlar ancak bir kurumsal ağ koruması yoksa, paylaşılan dosyalara erişim hiç istenmeye bazı sonuçlara yol açabilir. Bir sistemde depolanan tek bir virüslü dosya muhtemelen önemli iş, finans ve itibar zararına yol açarak tüm ağı tehlikeye atabilir. Bu nedenle ağ depolama sistemleri için kapsamlı bir koruma kesinlikle zorunludur.

Kaspersky Anti-Virus for Storage, EMC Celerra ürün çeşitleriyle tümüyle uyumludur. Celerra sistemlerinde depolanan dosyalara ve arşivlere en üst düzeyde korumanın, kötü amaçlı yazılımların tespiti ve etkisizleştirilmesi sağlanması için uzmanlarca tasarlanmıştır. Çözüm sistemi yöneticilerin tarama görevlerini nesneler kaydedilirken ve değiştirilirken veya gerekiyorsa, istek üzerine gerçek zamanlı olarak yapmasına olanak verir.

ÖZELLİKLER

- EMC Celerra veri depolama sistemleri için koruma
- Windows Server® 2008 R2 için destek
- Hiyerarşik Depolama Yönetim Sistemleri (HSM) için destek
- Yeni kötü amaçlı programlardan genişletilmiş ileriye etkili koruma
- Gerçek zamanlı olarak anti-virüs koruması
- Dosya depolarının zamanlanmış taraması
- Kritik sistem alanlarını tarama
- Sistem kaynaklarının optimizasyonu
- Temizleme veya silme işleminden önce verilerin yedek depolaması
- Ölçeklenebilirlik
- VMware Ready sertifikası
- Kaspersky Security Center ile merkezi kurulum, yönetim ve güncellemeler
- Kaspersky Endpoint Security for Business Platform ve diğer Kaspersky Ürünleriyle tam bütünleşir
- Uygulama durumu bildirim sistemi
- Ağ koruma durumunda kapsamlı raporlar

KASPERSKY SECURITY FOR MOBILE

Mobil Cihaz Yönetimi (MDM) ile Endpoint Security for Mobile Devices'ı birleştiren eksiksiz mobil güvenlik.

Kaspersky MDM mobil cihazların sorusuz ve kolay yapılandırmasını sağlarken Kaspersky Endpoint Security for Mobile Devices günümüzün tehditlerine karşı ihtiyaç duyduğunuz korumayı, çalışanların kendi cihazlarında bile sağlar.

KASPERSKY SECURITY FOR MOBILE'IN AYRINTILI ÖZELLİKLERİ:

BT ETKİLİLİĞİ ÖZELLİKLERİ:

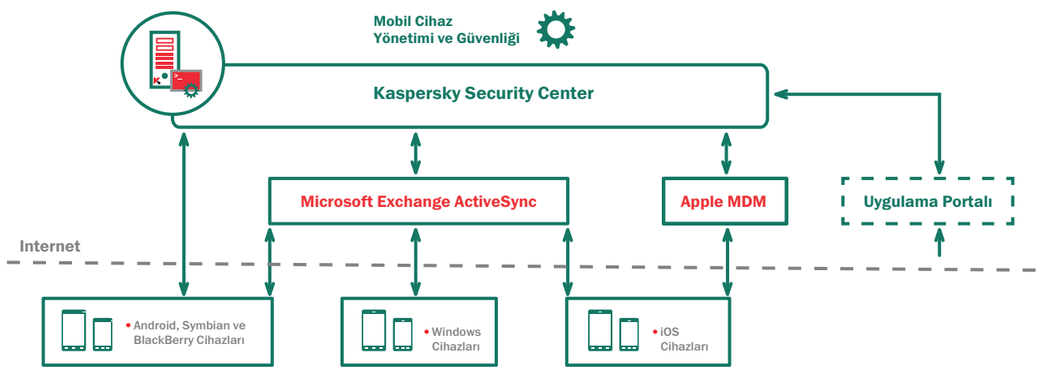
TEK KONSOLLA BASİT YAPILANDIRMA
Diğer çözümlerin aksine Kaspersky Lab yöneticilerin mobil cihazların, fiziksel uç noktaların, sanal sistemlerin, kriptolamanın ve ilke uygulama araçlarının güvenliğini yönetmek için yalnızca bir tek konsol kullanmasına imkan verir.

ÖZEL UYGULAMA PORTALI
Yöneticiler onaylanmış uygulamalara bağlantılar içeren kurumsal bir portal yayınlar. Kullanıcılar yalnızca bu uygulamalarla sınırlanabilir.

"KABLOSUZ" YAPILANDIRMA
Telefonları kullanıcıların onayladığınız profili ve uygulamaları indirebileceği kurumsal portala bir bağlantı içeren bir e-posta veya SMS göndererek uzaktan güvence altına alır. Kullanıcı kabul edene kadar verilere erişime izin verilmez.

GÜVENLİ YAPILANDIRMA
Rooting ve jailbreak işlemlerinin tespit edilmesini etkinleştirerek donanım ve yazılım bütünlüğünü sağlar. Diğer güvenlik ayarları 'kamerayı devre dışı bırakma', zorlanmış parola ve daha fazlasını içerir.

UYGUNLUK VE İLKE UYGULAMASI
Uygulama denetimi, 'Varsayılan Reddet' ve 'Varsayılan İzin Ver' desteği dahil cihazda uygulama kullanımının izlenmesine ve denetimine olanak verir.



GÜVENLİK RİSKİ DENETİMİ:

ŞİFRELEME
Hareket halindeki veriler, aynı zamanda bir taşıyıcıya uygulanabilecek açık tam disk ve dosya düzeyi veri kriptolama ile korunur.

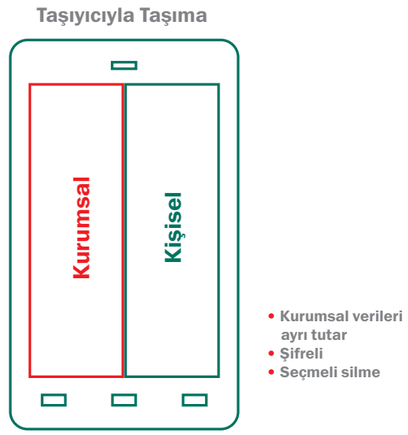
HIRSIZLIĞA KARŞI KORUMA
Bir SIM kartı çıkarılır veya değiştirilirse, yöneticiler tam veya seçmeli bir cihaz silme, GPS "Bul" işlevini kullanarak kayıp bir cihazın tam yerini bulma ve bildirim alma işlemlerini uzaktan gerçekleştirebilir.

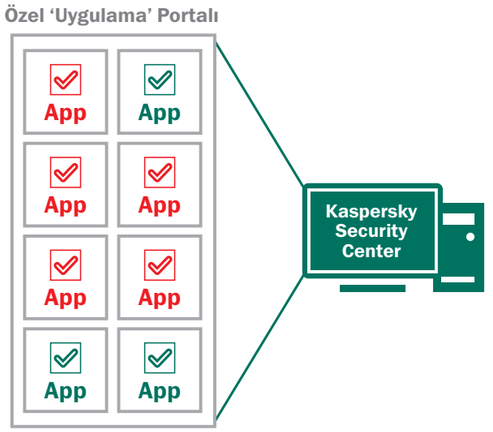
MOBİL KÖTÜ AMAÇLI YAZILIMA KARŞI KORUMA
Kaspersky Lab'ın kötü amaçlı yazılımdan koruma bulut destekli korumayı içeren çok katmanlı tespit özelliğine sahiptir ve cihazın kötü amaçlı yazılımlar tarafından tehlikeye düşürülmemesini sağlamak için güvenli bir tarayıcı ile güçlü istenmeyen posta korumasını birleştirir.

KURUMSAL VE KİŞİSEL VERİ BÜTÜNLÜĞÜ:

TAŞIYICILAR
Çalışanın kendi cihazı senaryosunu desteklemek için kurumsal veriler ve uygulamalar yalıtılmış "taşıyıcılara" yerleştirilebilir. Bu, kurumsal veriler için maksimum güvenlik ve kişisel içerik için optimum bütünlük sağlar.

UZAK VERİ GÜVENLİĞİ ARAÇLARI
Bir cihazın kaybolması durumunda, Uzaktan Kilitleme çalıştırılabilir. Cihazdaki bir taşıyıcıdaki kurumsal veriler, cihazdaki kişisel verilerden bağımsız olarak güvence altına alınabilir, şifrelenebilir, uzaktan yönetilebilir ve temizlenebilir.





"KENDİ CİHAZINI GETİR" (BYOD) İNİSİYATİFLERİ İÇİN MÜKEMMEL

Birçok çalışan hem kişisel hem de kurumsal görevler için kendi cihazlarını kullanır. Aslında, bazı kuruluşlar kullanıcıların bir perakende satıcıdan aldıkları, kendi tercihleri olan akıllı telefon veya tableti seçmelerini teşvik ediyor ve BT departmanı kullanıcının kendi cihazına e-posta ve kurumsal erişim ekliyor.

Bunda tasarruf ve verimlilik yararları vardır ancak BYOD beraberinde kuruluşu güvenlik risklerine açık kılabilir. Uygun şekilde korunmayan ve muhtemelen kişisel öğelerle karışmış kurumsal veriler kolayca istismar edilebilir. Bu cihazlar çoğu zaman, uygulama güvenliğine dikkat edilmeksizin aile fertleri tarafından da kullanılıyor. Hatta bazılarında root veya jailbreak işlemleri yapılmış oluyor.

Kaspersky Security for Mobile, ağ güvenliğinizdeki konsolun aynısını kullanarak akıllı telefonlar ve tabletlerin güvenli yapılandırmasını ve dağıtımını sağlayarak bu sorunları çözer. BT yöneticileri kullanıcı cihazlarının doğru ayarlarla yapılandırıldığından ve kaybolması, çalınması ve kullanıcı tarafından kötüye kullanılması durumunda güvence altına alabilir.

KASPERSKY SYSTEMS MANAGEMENT

Kaspersky Systems Management uygulamaya konuyor. Bu çözüm, aynı kodla yazılmış ve bir konsoldan yönetilen geniş bir güçlü BT üretkenliği araçları seti sunuyor. Ortaya çıkan platform istediğiniz basitliği ve otomasyonu ve ihtiyaç duyduğunuz güvenlik ve denetimi sağlıyor.

BİRBİRİNE BENZEMEYEN BT ARAÇLARI KARMAŞIKLIĞA NEDEN OLUR VE KARMAŞIKLIK GÜVENLİĞİN DÜŞMANIDIR.

İşi tekrar yapmaktan kaçının
Tekil sistemleri yeni ve mevcut kullanıcılar için tekrar kurma çabasını ortadan kaldırın. Sistem yapılandırma teknolojisini kullanarak merkezi bir yerden disk görüntüleri oluşturulup yönetilebilir ve dağıtılabilir.

Güvenliği arttırın
Yöneticiler bize günlerini genellikle yamaların güncel olmasını sağlamanın doldurduğunu anlatıyorlar. Kaspersky, hemen kötüye kullanılabilecek zayıf noktaları ve düzeltilmesi mesai sonrasına ertelenebilecek olanları tespit ederek karmaşıklığın giderilmesine yardımcı olur. Bu önceliklendirme yöneticilerin kendi günlerini planlamasına ve güvenlik pozisyonunu arttırmasına yardımcı olur.

Verimli çalışın
Yöneticiler görüntüleri, yamaları ve uygulamaları uzaktan kurabilir. Bir kullanıcının sorunu olduğunda BT makinede uzaktan oturum açarak sistemde sorunu giderebilir. Bu, yöneticinin masadan masaya taşınarak veya daha az üretken telefon desteği vermek için, işini engelleyen saatleri harcayarak zamanını tüketmemesi demektir.

Bu özellikler ve daha fazlası Kaspersky Systems Management'ın parçasıdır ve Kaspersky Security Center yönetim konsolu aracılığıyla erişilebilir. Her araç kendi konsolunu gerektirmediğinden ötürü, komutlar tutarlı ve sezgiseldir ve hiçbir ek eğitim gerektirmez.

SİSTEM YÖNETİMİ ÖZELLİKLERİ:

İŞLETİM SİSTEMİ VE UYGULAMANIN YAPILANDIRMASI
Sistem görüntülerinin merkezi bir yerden kolay oluşturulması, depolanması, klonlanması ve dağıtımı. Sistemlerin kullanıcıyla sorunsuz olarak ve optimum güvenlik ayarlarıyla teslim edilmesini sağlama. Bu araç Microsoft Windows 8'e taşıma için çok uygundur.

ZAYIF NOKTALARDAN UZAK KALIN
Bir tıklatmayla donanım ve yazılım taraması sonuçları birden fazla zayıf nokta veritabanında karşılaştırır, böylece hangi zayıf noktaların hemen ilgiye gerek duyduğuna ve hangilerini mesai sonrasına erteleyebileceğinize karar ve öncelik verebilirsiniz.

UZAK, ESNEK YAZILIM KURULUMU
Elle veya zamanlanmış dağıtımları kullanarak ağın iş yükünü en aza indirin.

UZAK ARACILAR
Uzak veya bir şube ofisindeki bir işistasyonunu merkezi güncelleme aracısı olarak atayın. Uzak bir ofise bir güncelleme göndererek ve atanan bir işistasyonunu güncellemeyi bu yerden dağıtmak için kullanarak bant genişliğini koruyun.

YEREL AĞDA AÇ (WAKE ON LAN) TEKNOLOJİSİ DESTEĞİ
Mesai dışı saatlerde dağıtım veya destek için, Kaspersky Systems Management bir iş istasyonunu uzaktan açabilir.

SORUN GİDERME ARAÇLARI
Sorunları gidermek için bir istemci sisteme aynı yönetim konsolundan uzaktan ve güvenli şekilde bağlanın.

MICROSOFT WINDOWS SUNUCUSU GÜNCELLEME HİZMETLERİ (WSUS) İÇİN DESTEK
Kaspersky Systems Management, Microsoft Windows güncellemeleri dahil, mevcut güncellemeler ve düzeltmeleri Windows Güncelleme Hizmetleri aracılığıyla indirip etkili şekilde dağıtarak verileri bunlarla düzenli olarak senkronize eder.

AĞ GİRİŞ DENETİMİ (NAC)
Ağ Giriş Denetimi (NAC) ile bir 'konuk' ilkesi oluşturabilirsiniz. Konuk cihazlar (mobil cihazlar dahil) otomatik olarak tanınır ve doğru kimlik parolasıyla, onayladığınız kaynakları kullanabilecekleri bir kurumsal portala gönderilirler.

DONANIM VE YAZILIM ENVANTERLERİ
PC'ler, sabit diskler ve hatta çıkarılabilir cihazlar otomatik olarak bulunur ve envantere eklenir. Ağ Giriş Denetimi (NAC) ile bir 'konuk' ilkesi oluşturabilirsiniz. Bu özellik yöneticinin ağdaki donanımların durumunu ve kullanımını izlemesini sağlar.

LİSANS TEDARİKİ VE DENETİMİ
Kaspersky Systems Management ortamınızda hangi yazılımların kullanıldığı tam olarak bildirir. Bu, lisans alma masraflarınızı ayarlamanızı ve uygun olmayan kullanıcıları belirlemenizi sağlar. Kaspersky Lab'ın uç nokta denetim araçlarıyla dağıtıldığında, kullanımı yalnızca onaylanmış uygulamalar ve sürümleriyle sınırlayabilir ve herhangi bir anda kullanımda olan lisans sayısını kısıtlayabilirsiniz.

KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server Microsoft® Windows®, Novell NetWare ve Linux ile çalışan sunucuları her türlü kötü amaçlı programlardan güvenilir şekilde korur.

Paylaşılan dosya deposu için anti-virüs koruması zorunludur ve bir sunucudaki tek bir virüslü dosya kaynağın tüm kullanıcılarının işistasyonlarına bulaşabilir. Dosya sunucusunun doğru şekilde korunması yalnızca kullanıcıların ve verilerinin korunmasını sağlamakla kalmaz, tekrarlanan kötü amaçlı yazılım salgınlarına ve diğer olaylara neden olabilecek, kötü amaçlı programların dosyalarının kopyalarını yedekleme tehlikesini de ortadan kaldırır.

ÜRÜNÜN ÖNEMLİ NOKTALARI*

- Microsoft® Windows® ve Linux platformlarının son sürümleri için destek
- Sistem kaynaklarının optimizasyonu
- Hiyerarşik Depolama Yönetim Sistemleri (HSM) için destek
- Terminal sunucuları ve küme sunucuları koruma
- VMware Ready sertifikası
- NSS dosya sistemi desteği
- Ücretsiz BSD desteği

ÖZELLİKLER

- Windows® (Windows Server® 2008 R2 dahil), Linux (Samba dahil) ve Novell NetWare ile çalışan dosya sunucularını koruma
- Yeni kötü amaçlı programlardan genişletilmiş ileriye etkili koruma
- Gerçek zamanlı olarak anti-virüs koruması
- Etkin virüs bulaşmalarını temizleme
- Dosya depolarının zamanlanmış taraması
- Kritik sistem alanlarını tarama
- Virüslü işistasyonlarını yalıtma
- Ölçeklenebilirlik
- Temizleme veya silme işleminden önce verilerin yedek depolaması
- Merkezi kurulum, yönetim ve güncellemeler
- Kurulum ve yönetim yöntemleri seçenekleri
- Tarama ve olay yanıtlama senaryoları için esnek bir sistem
- Uygulama durumu bildirim sistemi
- Ağ koruma durumunda kapsamlı raporlar

UYGULAMALAR

- Kaspersky Anti-Virus for Windows® Servers Enterprise Edition
- Kaspersky Anti-Virus for Linux File Server
- Kaspersky Endpoint Security for Windows®
- Kaspersky Anti-Virus for Novell NetWare
- Kaspersky Security Center

* Ürün özellikleri kullanılan bileşenlerin bileşimine bağlı olarak değişebilir. Bileşen açıklamaları için lütfen şu adrese bakın: www.kaspersky.com.tr

KASPERSKY SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server posta ve grup yazılımı sunucularını kötü amaçlı programlara ve istenmeyen postalara karşı korur.

Ürün Microsoft® Exchange, Lotus® Domino®, Sendmail, Qmail, Postfix, Exim ve CommuniGate Pro dahil tüm popüler sunucular için posta trafiğini koruyan uygulamaları içerir. Çözüm özel bir ağ geçidi ayarlamak için de kullanılabilir.

ÜRÜNÜN ÖNEMLİ NOKTALARI*

POSTA SUNUCUSU KORUMASI
Tüm popüler posta sistemleri için posta trafiğini kötü amaçlı yazılıma karşı koruma ve anti-spam.

SİSTEM KAYNAĞI OPTİMİZASYONU
Yeni bir anti-virüs motoru, sunucu kaynaklarının yük dengelemesi ve tarama istisnalarının hepsi sisteminizdeki yükü azaltır.

ANTI-SPAM İÇİN KSN BÜTÜNLEŞTİRMESİ
Kaspersky Lab'ın bulut tabanlı tehdit tespit motoru (KSN) ile bütünleşme sayesinde istenmeyen postaların tespit edilme oranını arttırır.

AZALTILMIŞ TRAFİK YÜKÜ
Bulut etkin, akıllı istenmeyen posta filtreleme trafik yükünü önemli ölçüde azaltır.

ÖZELLİKLER

- Posta sunucularını her türden kötü amaçlı programa karşı bütünlemiş koruma
- İstenmeyen postalara karşı etkili koruma
- Gerçek zamanlı anti-virüs koruması
- E-postaların ve veritabanlarının zamanlanmış taraması
- Sendmail, qmail, Postfix, Exim ve CommuniGate Pro posta sunucuları için koruma
- Lotus® Domino® sunucularındaki mesajları, veritabanlarını ve diğer nesneleri tarama
- Ortak klasörler dahil, Microsoft® Exchange sunucusundaki tüm mesajları tarama
- Mesajları ek türlerine göre filtreleme
- Ölçeklenebilirlik
- Microsoft® Exchange Server 2007 kümeleri ve DAG for Microsoft® Exchange Server 2010 desteği
- Temizleme veya silme işleminden önce verileri yedekleme deposu
- Virüslü işistasyonlarını yalıtma
- Tekrarlanan posta taramayı iptal etme
- Kurulum yönetimi ve güncellemeler için uyun araçlar
- Koruma durumu hakkında kapsamlı raporlar
- Esnek tarama sistemi ve olay yanıtlama senaryoları
- Uygulama durumu bildirim sistemi

UYGULAMALAR

- Kaspersky Security for Microsoft® Exchange Servers
- Kaspersky Anti-Virus for Lotus® Domino®
- Kaspersky Security for Microsoft® Exchange Server 2003
- Kaspersky Security for Linux Mail Server

* Ürün özellikleri kullanılan bileşenlerin bileşimine bağlı olarak değişebilir. Bileşen açıklamaları için lütfen şu adrese bakın: www.kaspersky.com.tr adresinden tekil bileşen özellikleri hakkında daha fazla bilgi alabilirsiniz.

KASPERSKY SECURITY FOR VIRTUALIZATION

Sanallaştırılmış BT ortamlarının benzersiz ihtiyaçları için geliştirilen Kaspersky Security for Virtualization sanallaştırılmış sunucular, masaüstü bilgisayarlar ve veri merkezleri için ödüllü bir kötü amaçlı yazılımlardan koruma sunar.

Kaspersky Security for Virtualization sanallaştırılmış altyapınızı daha yüksek bir performansla ve sanallaştırma yoğunluğuna daha az etkiyle korumak için daha etkili bir sağlayan aracısız bir kötü amaçlı yazılımlardan koruma çözümüdür. Uygulamanın dağıtılması kolaydır ve hem fiziksel ham de sanal bilişim varlıklarında ki çok çeşitli güvenlik görevlerini basitleştiren gelişmiş yönetim özelliklerine sahiptir.

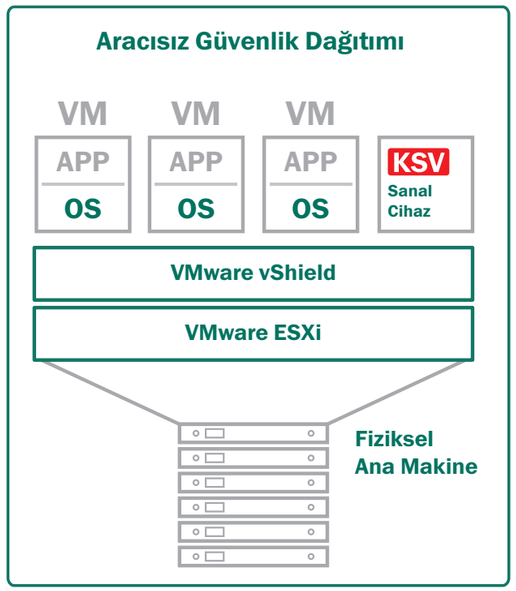
KORUMA VE PERFORMANS ÖZELLİKLERİ

- Merkezi güvenlik. Kaspersky Security for Virtualization kötü amaçlı yazılıma karşı tarama becerilerini sunmak için VMware's vShield Endpoint'a bağlanan sanal bir cihazdır. Her fiziksel ana makine için kötü amaçlı yazılıma karşı tek bir merkezi motor ve veritabanı sağlar.

- Gelişmiş Anti-Virüs Motoru. Kaspersky'nin ödüllü kötü amaçlı yazılımdan koruma teknolojileri Kaspersky'nin sektörün öncüsü güncelleme sıklığıyla birlikte yeni ve ortaya çıkan tehditlerden korunmayı sağlar. Sezgisel bir çözümleyici çok biçimli kötü amaçlı yazılımlarla mücadele eder.

- Otomatik Koruma. Güvenlik açıklarını ve yanlış yapılandırmaları ortadan kaldırmak için kötü amaçlı yazılımdan koruma yeni sanal makinelere otomatik olarak sağlanır. Tüm konuk VM'ler, önceden çevrimdışı olmasına bakılmaksızın her zaman en son imza veritabanıyla korunur.

- Daha yüksek yoğunluklu sanallaştırma. Kaspersky Security for Virtualization aracısız bir çözüm olduğu için, 'Güncelleme Fırtınaları' ve 'Tarama Fırtınaları'nı ortadan kaldırmaya, yüksek yoğunluklu sanallaştırmaların gerçekleştirilmesine, performansa etkisinin azaltılmasına ve bazı aracı tabanlı ürünlerin oluşturabileceği güvenlik açıklarının yanıtlanmasına yardımcı olur.



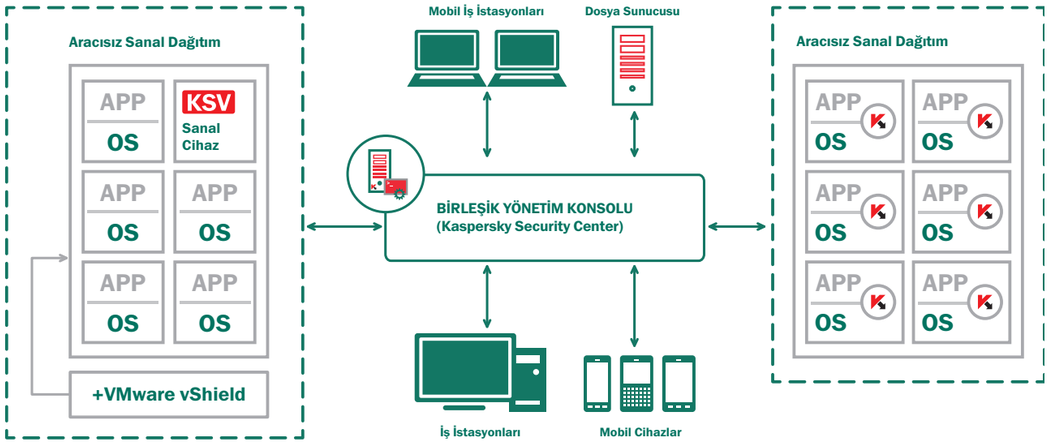
Kaspersky Security for Virtualization, VMware dağıtımları için aracısız virüsten koruma sağlar.

YÖNETİM ÖZELLİKLERİ:

TEK YÖNETİM KONSOLU.
Hiçbir ek masraf olmaksızın kullanılabilecek Kaspersky Security Center sanal makinelerin, fiziksel makinelerin ve mobil cihazların güvenliğini yönetmenize olanak veren tek bir yönetim konsoludur.

VMWARE VMOTION'I DESTEKLER.
VMware vMotion'ı tümüyle destekleyen Kaspersky Security for Virtualization bir iş yükü bir ESXi ana makinesinden bir başkasına taşındığında korumanın kesintiye uğramamasını sağlar. Yeni ana makinenin gerekli lisanslara sahip olmayı kaydıyla, koruma iş yükünü izleyecek ve tüm güvenlik ayarları aynı kalacaktır.

VMWARE VCENTER İLE BÜTÜNLEŞMİŞ.
Kaspersky Security for Virtualization, tüm sanal makinelerin ve ilgili parametrelerin bir listesini de içeren, sanal makineler hakkındaki bilgileri vCenter'dan alır. vCenter ile bu bütünleştirme, BT ekibine en iyi görünürlüğü sağlamaya ek olarak, yeni bir sanal makine yapılandırıldığında korumanın otomatik olarak verilmesini sağlar.



KSV Kaspersky Security for Virtualization

Kaspersky Lab Security Solution

KASPERSKY SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway bir kuruluşun tüm çalışanlarına güvenli İnternet erişimi sağlar.

Kaspersky Security for Internet Gateway, Windows ve Linux platformlarına dayalı en popüler ağ geçitlerini destekler. HTTP, HTTPS, FTP, POP3 ve SMTP protokolleri aracılığıyla çalıştığı bilinen kötü amaçlı ve potansiyel olarak tehlikeli programlar otomatik olarak veri akışından silinir. Optimizasyon teknolojisi, ölçeklenebilirlik ve en yeni platformlar için destek yüksek miktarlarda trafiği olan büyük kuruluşlar için idealdir.

ÜRÜNÜN ÖNEMLİ NOKTALARI*

- Microsoft® Forefront® TMG koruması
- Çok çeşitli ilke yönetimi ve yapılandırma araçları
- VPN bağlantılarını tarama
- E-posta trafiği koruması (POP3 ve SMTP protokolleri aracılığıyla)
- Yayınlanan sunuculardan HTTP ve FTP trafiğini tarama
- VMware Ready sertifikası

ÖZELLİKLER

- HTTP, HTTPS, FTP, POP3 ve SMTP protokollerini kullanarak internet trafiğini gerçek zamanlı tarama
- Her türden kötü amaçlı programa karşı bütünlemiş koruma
- Squid, Blue Coat ve Cisco® proxy sunucuları için destek
- Yedekleme deposu
- Sunucu işlemlerinin yük dengelemesi
- Ölçeklenebilirlik
- Kurulum yönetimi ve güncellemeler için uygun araçlar
- Esnek tarama sistemi ve olay yanıtlama senaryoları
- Ağ koruma durumunda kapsamlı raporlar

UYGULAMALAR

- Kaspersky Anti-Virus for Microsoft® ISA Server and Forefront® TMG Standard Edition
- Kaspersky Anti-Virus for Microsoft® ISA Server Enterprise Edition
- Kaspersky Anti-Virus for Proxy Server

* Ürün özellikleri kullanılan bileşenlerin bileşimine bağlı olarak değişebilir. Bileşen açıklamaları için lütfen şu adrese bakın: www.kaspersky.com.tr adresinden tekil bileşen özellikleri hakkında daha fazla bilgi alabilirsiniz.

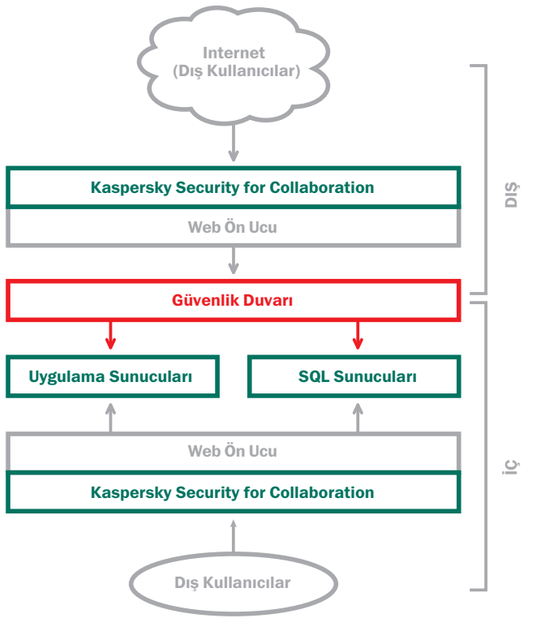
KASPERSKY SECURITY FOR COLLABORATION

Kaspersky Security for Collaboration, yönetim kolaylığını ve kötü amaçlı yazılımlardan yüksek korunma oranlarını birleştirerek en son koruma teknolojilerini Birlikte Çalışma platformunuza uygular.

Kaspersky Security for Collaboration, Microsoft® SharePoint® ortamlarını korumak için Kaspersky'nin ödüllü anti-virüs motorunu kullanır. Bu ürün, ödüllü kötü amaçlı yazılımlardan koruma teknolojisiyle tek bir sunucuyu veya SharePoint çiftliklerinin tümünü korurken içerik ve dosya filtreleme yetenekleri uygunsuz içeriğin depolanmasının engellenmesine yardımcı olur.

ÖZELLİKLER

- Yükleme indirme denemelerinden gelen tehditleri gerçek zamanlı olarak tespit edip engellemek üzere tasarlanmış yenilikçi tespit teknolojisi
- Son kullanıcıların belirtilen dosya türlerini (örneğin müzik, video dosyaları, yürütülebilir dosyalar) veya uygun olmayanmetinleri depolamasını engeller
- Genel yönetim ayarları tek bir gösterge tablosundan tüm korunan sunucularda yapılandırılabilir
- Hiçbir özel eğitim gerektirmeyen, basit, sezgisel yönetim
- Active Directory ile bütünleşme kurulum ve kullanıcının kimlik doğrulamasını kolaylaştırır
- Ayrıntılı günlükler ve değiştirilmiş dosyaların yedeklenmesi yöneticilerin ihlalleri veya güvenlik sorunlarını yanıtlamasına yardımcı olur
- Ayrıntılı, esnek raporlama



KASPERSKY SMALL OFFICE SECURITY

Kaspersky Small Office Security küçük işyerleri için özel olarak tasarlanmıştır. Kurulumu, yapılandırılması ve kullanımı kolay, çok düşük maliyetli, dünya sınıfı PC ve sunucu koruması sunar.

Kaspersky Small Office Security BT uzmanları gerektirmeyen dünya sınıfı BT güvenliği sağlar. Kurulması kolaydır, sistemi yavaşlatmaz ve işletmenizi her türden tehdide ve kötü amaçlı yazılıma bağışık kılar. Dijital çalışma alanınızı işletmeniz için mümkün olan en iyi korumayla sağlıklı durumda tutar.

ÖZELLİKLER

- Virüslere, casus yazılımlara ve Truva atlarına ve daha fazlasına karşı gerçek zamanlı koruma
- Çalışanların internet sitelerine, uygulamalara, oyunlara ve sosyal ağlara erişimini sınırlama
- Zamanlanmış ve otomatik yedeklemelerle iş verilerinize tam koruma sağlama
- Verileri e-posta veya USB sürücüsü aracılığıyla güvenli şekle aktarılabileceği şifreli kasalarda depolama
- Siz ve çalışanlarınız için kırılması zor parolalar üretme ve güvenli şekilde depolama *
- Sık güncellemelerle ve dikkat çekmeyen işlemlerle maksimum sistem performansını sağlama
- Bilgisayar korsanı saldırılarını anında engelleyen gelişmiş teknolojiler
- WiFi dahil işletmenin BT ağı güvenliğinin ince ayarı için araçlar
- Hassas veri geri yüklenemeyecek veya çalınamayacak şekilde silen Dosya Parçalayıcı yardımcı programı

YÖNETİM

- Tek bir PC'den merkezi ağ güvenliği yönetimi
- Basit, sezgisel arabirim
- Gelişmiş ağ güvenliği için geliştirilmiş kolay yönetim
- Web kullanım ilkesi yönetimi

İÇİNDEKİ UYGULAMALAR

Kaspersky Small Office Security'nin desteklediği platformlar / işletim sistemleri:

- Microsoft® Windows® (Microsoft® Windows® 7 dahil)
- Windows® Sunucuları (Windows Server®2008R2 dahil)

Kaspersky Lab Türkiye
www.kaspersky.com.tr

İnternet güvenliği hakkında
her şey: www.securelist.com

Size yakın bir iş ortağını bulun:
www.kaspersky.com/buyoffline