



Kaspersky®  
Security  
for Mail Server

# İş e-postaları için Başarısını Kanıtlamış Yeni Nesil koruma

E-posta, kurumsal BT güvenliğini tehdit eden bir numaralı kötü amaçlı yazılım vektörüdür.<sup>1</sup> Kaspersky Security for Mail Server, e-postaları fidye yazılımlara, kötü amaçlı eklere, istenmeyen e-postalara, kimlik avı saldırılarına ve bilinmeyen tehditlere karşı korumak için gelişmiş sezgisel algoritmalar, korumalı alan teknolojisi, makine öğrenimi ve diğer Yeni Nesil teknolojileri kullanır.

Dünyanın en çok test edilen ve en çok ödül alan güvenliği ile işletmenizi, e-posta tabanlı saldırıların neden olduğu finansal ve operasyonel kayıplardan ve itibar kayıplarından koruyun.

## Avantajlar

**Gönderilen tüm e-postaların yarısından fazlası istenmeyen e-postalardan oluşur. Yeni Nesil istenmeyen e-posta koruması ile verimliliği artırın ve tehditleri azaltın**

Kaspersky Lab'in istenmeyen postalara karşı bulut destekli Yeni Nesil koruması, hatalı pozitifler nedeniyle değerli e-postaların silinmesini minimum düzeye indirirken en gelişmiş ve bilinmeyen e-posta saldırılarını bile tespit eder. Bu çözüm, istenmeyen e-postaları, size ulaşmadan önce durdurarak bu postalar için harcanan zamanın ve kaynakların yanı sıra ilgili risklerin de azalmasına yardımcı olur. Bu sayede sistem ve insan kaynaklarınızdan tasarruf edebilirsiniz.

### Düşük sahip olma maliyeti

Kaspersky Security for Mail Server, yönetebilirliği ve kullanım kolaylığını dengeleyerek BT personelinin diğer görevler için zaman ayırmasını sağlar. Esnek filtreleme yapılandırma senaryoları, iş süreçlerinize mükemmel bir şekilde uyum sağlayarak yönetim kaynaklarını azaltır.

### Küçük ve Orta Ölçekli İşletmeler için esnek ödeme seçenekleri

Kaspersky Security for Mail Server, yıllık lisans veya uygun aylık abonelik lisansı ile sağlanabilir.

### Yönetilen Hizmet Sağlayıcıları (MSP'ler) İçin Kolaylık

Gittikçe daha çok sayıda MSP, siber güvenliği değer önermesine eklemektedir. Kaspersky Security for Mail Server, bir MSP destek hizmetinin ihtiyaç duyabileceği çok kiracılı yönetim özelliğini, esnek lisans seçeneklerini ve doğru sistem sağlık raporlama biçimini destekler.

### Önemli Özellikler

- Kötü amaçlı yazılımlara karşı gerçek zamanlı ve isteğe bağlı Yeni Nesil koruma
- Kaspersky Anti Targeted Attack Platform (KATA) ile iki yönlü entegrasyon
- Kimliği doğrulanmış e-posta yönetimi, Kurumsal E-postaların Ele Geçirilmesi (BEC) saldırılarıyla mücadele etmeye yardımcı olur
- Son kullanıcılar ve MSP'ler için aylık abonelik lisansı ile kullanılabilir
- Sıfır gün tehditlerine karşı koruma
- Kaspersky Security Network'ten global tehdit istihbaratı tarafından desteklenmektedir
- LDAP/Microsoft Active Directory desteği
- E-postalar ve ekler için karantina yönetimi
- Gömülü kötü amaçlı makrolarla ve diğer nesnelere ilişkin
- E-posta ile dağıtılan fidye yazılımlarını durdurur

<sup>1</sup> Verizon Veri İhtali İnceleme Raporu 2017.

# Özellikler

## Kötü amaçlı yazılımlara karşı HuMachine™ destekli ve çok katmanlı koruma

Kaspersky'nin Yeni Nesil kötü amaçlı yazılımlara karşı koruma işlevi, gelen e-postalardaki kötü amaçlı ekleri, bilinen ve bilinmeyen kötü amaçlı yazılımları filtrelemek için makine öğrenimi ve bulut destekli tehdit istihbaratı dahil olmak üzere birden çok proaktif güvenlik katmanı içerir. Gerçek zamanlı ve isteğe bağlı tarama kullanılabilir. Isteğe bağlı tarama, özellikle geçiş senaryoları için kullanışlıdır.

### Global tehdit istihbaratı:

Kaspersky Security for Mail Server, sürekli gelişen tehdit ortamının son halini görmek için dünyanın dört bir tarafından toplanan verileri kullanır.

#### • Makine öğrenimi:

Global tehdit istihbaratından oluşan büyük veri, makine öğrenimi algoritmalarının ve insan uzmanlığının birleşimi tarafından işlenerek minimum sayıda hatalı pozitif sonuç veren başarısını kanıtlamış yüksek tespit düzeyi sunar.

#### • Korunmalı alan emülasyonu:

E-posta ekleri, en karmaşık ve en gizli kötü amaçlı yazılımlara karşı koruma sağlamak için güvenli bir emülasyon ortamında yürütülür. Tehlikeli numunelerin kurumsal sisteme giriş yapmadığından emin olmak için ekler bu ortamda analiz edilir.

## Otomatik istenmeyen postalara karşı koruma sistemi (içerik bilinirliği özelliği)

Kaspersky'nin istenmeyen e-postalara karşı koruma sistemi, makine öğrenimi tabanlı tespit modellerini yoğun olarak kullanır. Hatalı pozitif sonuç olasılığını en aza indirmek ve tehdit ortamındaki değişikliklere uyum sağlamak için otomatik işleme, Kaspersky HuMachine™ sisteminin bir parçası olan Kaspersky Lab uzmanları tarafından denetlenir.

## Kimlik avı saldırılarına karşı gelişmiş koruma

Kaspersky'in Kimlik avı saldırılarına karşı gelişmiş koruma sistemi, etkili tespit modelleri için Yapay Sinir Ağları analizini temel alır. Resimler, dil denetimleri, özel komut dizileri dahil olmak üzere 1000'den fazla kriter kullanan bu bulut

destekli yaklaşım, bilinen ve bilinmeyen/sıfır gün kimlik avı e-postalarına karşı koruma sağlamak için kötü amaçlı ve kimlik avına yönelik URL'lerle ilgili dünyanın dört bir tarafından gelen verilerle desteklenir.

## Kimliği doğrulanmış e-posta yönetimi

SPF/DKIM/DMARC gibi güvenilir gönderen kimlik doğrulama mekanizmaları, kaynak sahtekarlığına karşı koruma sağlar. Bu işlev, özellikle Kurumsal E-postaların Ele Geçirilmesi (BEC) senaryoları için kullanışlıdır.

## Ek filtreleme

Bazı ek türleri, kurumsal güvenlik çevresine giremeyecek kadar risklidir. Kaspersky'nin ek filtreleme sistemi, ek alma ilkesinin esnek bir şekilde yapılandırılmasına olanak tanır ve siber suçlular tarafından yaygın olarak kullanılan birden çok dosya gizleme türünü tespit eder. Bu özellikler, veri sızıntısı olasılığını azaltmaya yardımcı olur.

## Dahili yedekleme

Temizleme veya silme nedeniyle önemli verilerin kaybolmasını önlemek için asıl iletiler, uygun olduğunda yönetici tarafından işlenmesi için yedek depolama alanına kaydedilebilir. Koşullu veri yedeklemesi için özel kurallar yapılandırılabilir.

## Kaspersky Anti Targeted Attack entegrasyonu

Kaspersky'nin güçlü Gelişmiş Kalıcı Tehditlere Karşı Koruma/ EDR çözümü ile iki yönlü entegrasyon, yalnızca posta sistemlerinin hedefli saldırı tespiti için ek bilgi kaynağı olarak kullanılmasını sağlamaz aynı zamanda KATA derin analizinin sonuçlarına göre tehlikeli içeriğe sahip iletilerin engellenmesini geliştirir.

### Kaspersky HuMachine™ Yaklaşımı

Büyük Veri tehdit istihbaratından, otomatik makine öğrenimi becerilerinden ve uzmanların deneyiminden güç alan Kaspersky HuMachine™, birçok avantaj sunar ve daha etkili bir koruma sağlar. Birbirinden ayrı bileşenler, her bir unsurun birleştirilmesiyle daha etkili ve verimli bir bütün haline gelir.

2 Kaspersky Security for Microsoft Exchange Servers için Veri Sızıntısı Önlemem isteğe bağlı işlevi, ayrı olarak satın alınır.

### İçindeki uygulamalar

- Kaspersky Security for Linux Mail Server
- Kaspersky Security for Microsoft Exchange Server
- Kaspersky Anti-Virus for Lotus Notes/Domino
- Kaspersky Security Center

### Nasıl satın alınır?

Kaspersky Security for Mail Server çözümleri, yıllık lisans veya uygun aylık abonelik lisansı ile sağlanabilir. Ayrı olarak veya Kaspersky Total Security for Business çözümünün parçası olarak satın alınabilir.<sup>2</sup> E n uygun ürünü seçmenize yardımcı olması için lütfen Kaspersky satıcınıza veya yetkili distribütöre danışın.

[www.kaspersky.com.tr](http://www.kaspersky.com.tr)  
[#truecybersecurity](https://twitter.com/truecybersecurity)

© 2017 AO Kaspersky Lab. Tüm hakları saklıdır. Tescilli ticari markalar ve hizmet markaları ilgili sahiplerinin mülkiyetindedir.

