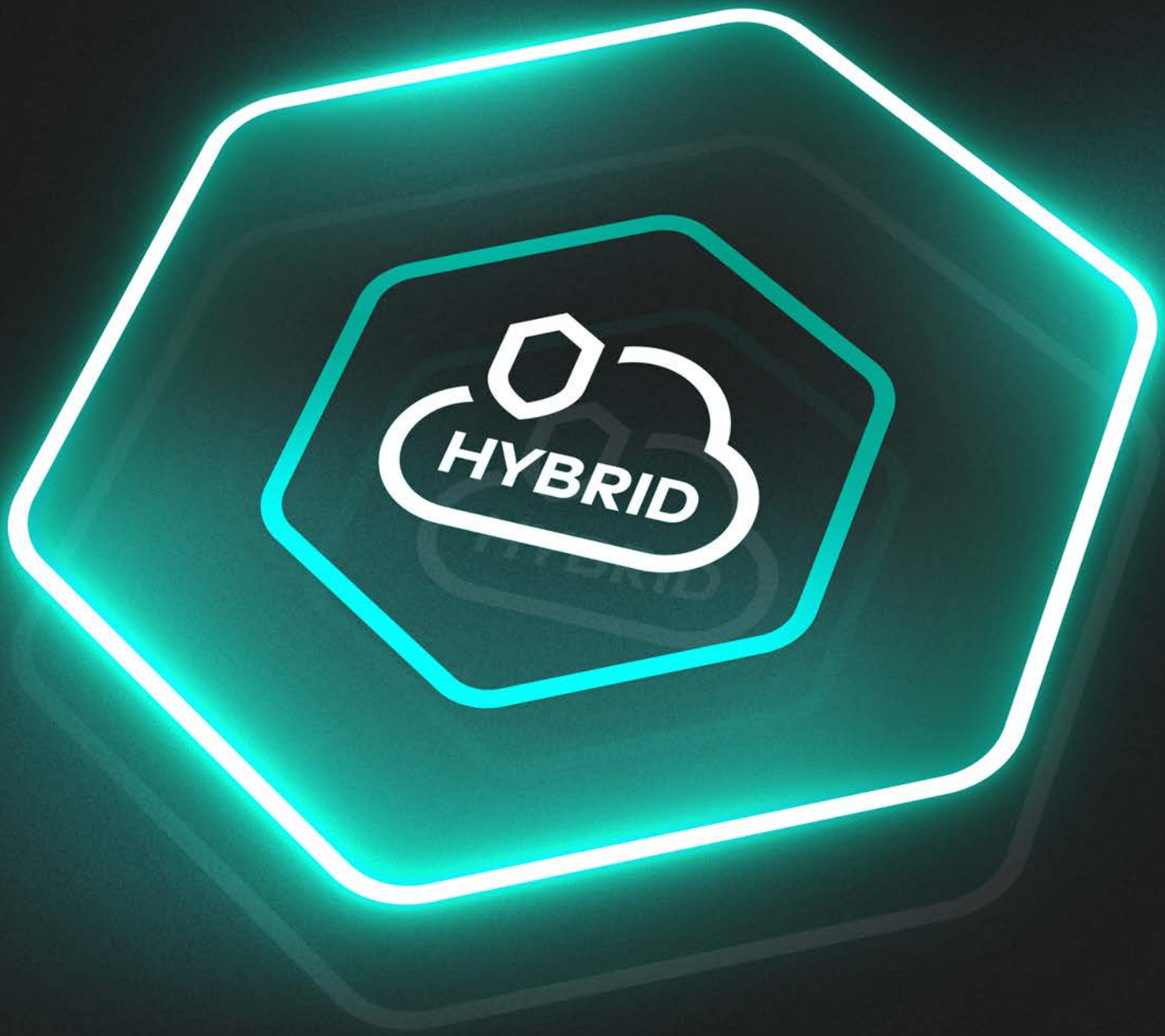


Kaspersky Hybrid Cloud Security

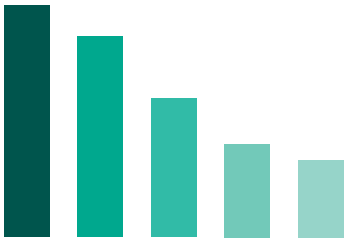
kaspersky GELECEĞİ YAKALAYIN

Günümüzde işletmelerin dijital dönüşüme odaklanması, bulutun hızla benimsenmesini sağlıyor. Bir yandan, bu girişimler işletmeler için daha fazla verimlilik dâhil olmak üzere birçok avantaj sunuyor. Diğer yandan ise altyapılar daha karmaşık hâle geliyor ve güvenlik riski, denetim, personel kaynakları, performans optimizasyonu, yeni yönetmelikler ve masraflar açısından önemli endişeler yaratıyor. Kaspersky Hybrid Cloud Security tüm bu sorunları ele alıyor.

Hibrit ortamlarınız için kanıtlanmış özel koruma ve en iyi performans

Kaspersky Hybrid Cloud Security; bulutun benimsenmesini, dijital dönüşümü ve genel olarak iş yapmayı daha güvenli ve verimli hâle getirir. Bu tek ürün, tüm hibrit altyapınızı güvence altına alarak riski azaltır, sanallaştırma kaynaklarının tüketimini azaltır ve yönetmeliklerle uyumu destekler. Kaspersky Hybrid Cloud Security, daha fazla görünürlük ve basitleştirilmiş yönetim sunarken sizin ve ekibinizin değerli zaman ve bütçe kaynaklarından tasarruf sağlar. Güvenlik, endişelenecek bir şey olmaktan çıkar ve sizi dijital dönüşüm yolculuğunuzun diğer yönlerine odaklanma konusunda özgür kılar.

Önemli bulut zorlukları



- Güvenlik **%81**
- Bulut harcamalarını yönetme **%79**
- Denetim ve Uyumluluk **%75**
- Çoklu bulut sistemini yönetme **%72**
- Bulut geçişi **%71**

Flexera'nın 2021 State of the Cloud Raporu'na göre

Hibrit ortam güvenlik risklerini ele almak üzere tasarlanmış türünün en iyisi koruma

- Çok katmanlı tehdit koruması; kötü amaçlı yazılım, kimlik avı ve daha fazlasını içeren en geniş kapsamlı siber saldırılarla proaktif olarak savaşır.
- İnsan uzmanlığıyla desteklenen makine öğrenimi algoritmaları, minimum oranda hatalı pozitif sonuç ile en yüksek algılama düzeylerini sunar.
- Gerçek zamanlı tehdit istihbaratı verileri, en son güvenlik açıklarına karşı savunma oluşturmaya yardımcı olur.

En iyi hibrit altyapı güvenliği performansı için buluta özel bir yaklaşım

- Siber güvenlik motoru; iş yükünün fiziksel, sanallaştırılmış veya özel, herkese açık ve hibrit bulut tabanlı olmasına bakılmaksızın tüm hibrit altyapıyı korur.
- Yerel entegrasyonla birleştirilen platformdan bağımsız yaklaşım, herkese açık bulut ortamlarını tamamen DevOps özellikli hâle getirir.
- Her işletim sistemi için optimize edilmiş hafif aracılar, sanallaştırma kaynaklarının tüketimini %30'a kadar verimli bir şekilde azaltarak diğer iş operasyonlarında kullanılmalarını sağlar.

Rahat bir bulut yolculuğu için uygun maliyetli ve kolay yönetim

- Esnek bir lisanslandırma modeli, sadece ihtiyacınız olan özellikleri seçerek güvenlik bütçenizden en iyi şekilde faydalanacağınız anlamına gelir.
- Bir birleşik bulut konsolu, tüm altyapınızda güvenlik yönetimini kolaylaştırarak değerli BT personeli kaynaklarından tasarruf etmenizi sağlar.
- Aracıların konumundan bağımsız olarak, doğrudan bulut altyapısı envanteri ve otomatik güvenlik sağlama, maksimum görünürlüğe katkıda bulunur.

Yüksek düzeyde denetime tabi sektörler için uyumluluğa hazır güvenlik

- Uyarlanabilir ve çok yönlü olan bu ürün, sistem güçlendirme ve aracı öz savunmasından güvenlik açığı değerlendirmesine ve otomatik yama yönetimine kadar değişen teknolojiler aracılığıyla yönetmeliklere tam uyumluluğu sağlamak ve sürekli olarak desteklemek için tasarlanmıştır.
- Geniş özellik yelpazesi, güvenliğinizin her zaman güncel mevzuatların kontrolünde olmasını sağlayarak uyumluluk ve risk ortamına uyum sunar.

Özellikler

Çok katmanlı tehdit koruması

Küresel Tehdit İstihbaratı	Tehdit alanının durumu değişirken bile bununla ilgili gerçek zamanlı verileri toplar.
Makine Öğrenimi	Makine öğrenimi algoritmaları ve insan uzmanlığı ile küresel tehdit istihbaratının büyük hacimli verilerini güçlendirir.
Web ve E-posta Tehdidi Koruması	Sanal ve uzak masaüstlerini güvende tutarak e-posta ve web tabanlı tehditlere karşı koruma sağlar.
Günlük Denetimi	En iyi çalışma hijyeni için günlük dosyalarını tarar.
Davranış Analizi	Uygulamaları ve süreçleri izleyerek dosyasız veya komut dosyası tabanlı kötü amaçlı yazılımlar dâhil olmak üzere gelişmiş tehditlere karşı koruma sağlar.
Düzeltme Motoru	Gerektiğinde bulut iş yüklerindeki kötü amaçlı değişiklikleri geri alır.
Açık Önleme	Korumalı uygulamalarla tam uyumluluk içinde tehdit sızmasına karşı etkili koruma sunarak performans üzerinde minimum etki sağlar.
Fidye Yazılımı Koruması İşlevselliği	Uzaktan başlatılan şifrelemenin engellenmesi ve etkilenen dosyaların önceden şifrelenmiş durumlarına geri döndürülmesi de dâhil olmak üzere iş açısından kritik verileri fidye olarak tutmaya yönelik her türlü girişimden korur.
Ağ Tehdit Koruması	Bulut tabanlı varlıklara ağ tabanlı izinsiz girişleri algılar ve önler.
Kapsayıcı Koruması	Virüslerin, güvenliği ihlal edilmiş kapsayıcılar aracılığıyla hibrit BT altyapısına taşınmasını önler.

Dayanıklılığı artıran sistem güçlendirmesi

Uygulama Denetimi	En iyi sistem güçlendirmesi için tüm hibrit bulut iş yüklerinin Varsayılan Olarak Reddet modunda kilitlenmesine ve çalışan uygulamaları yalnızca yasal ve güvenilir olanlarla sınırlandırılmasına izin verir.
Cihaz Kontrolü	Ayrı ayrı bulut iş yüklerine hangi sanal cihazların erişebileceğini belirler.
Web Kontrolü	Sanal ve uzak masaüstleri tarafından web kaynaklarının kullanımını düzenleyerek riski azaltır ve üretkenliği artırır.
Ana Bilgisayar Tabanlı İzinsiz Giriş Önleme Sistemi (HIPS)	Başlatılan uygulamalara güven kategorileri atarak bunların kritik kaynaklara erişimini kısıtlar ve yeteneklerini sınırlar.
Dosya Bütünlüğünü İzleme	Kritik sistem bileşenlerinin ve diğer önemli dosyalarının bütünlüğünü sağlamaya yardımcı olur.
Güvenlik Açığı Taraması ve Yama Yönetimi	Güvenlik açığı taraması, yama ve güncelleme dağıtımı, envanter yönetimi ve uygulama sunumları gibi temel güvenlik, sistem yapılandırması ve yönetim görevlerini merkezîleştirir ve otomatik hâle getirir.

Sınırsız görünürlük

Birleşik Güvenlik Yönetimi	Tüm altyapıya yönelik uç nokta ve sunucu koruması; ofiste, veri merkezinizde ve bulutta tek bir konsol üzerinden yönetilebilir.
Bulut API'si	Herkese açık ortamlarla sorunsuz entegrasyon; altyapı keşfi, otomatikleştirilmiş güvenlik aracısı dağıtımı ve ilke tabanlı yönetimin yanı sıra daha kolay envanter ve güvenlik sağlama olanağı sunar.
Esnek Yönetim Seçenekleri	Çok kullanıcılı özellikler, izin tabanlı hesap yönetimi ve rol tabanlı erişim kontrolü, tek bir sunucudan birleşik düzenlemenin avantajlarını korurken esneklik sağlar.
SIEM Entegrasyonu	Hibrit BT ağı genelinde kurumsal siber güvenliğin farklı yönlerini tek bir yerde bir araya getirerek Güvenlik Bilgi ve Yönetim Sistemi ile ürün entegrasyonuna olanak tanır.

Neden Kaspersky Hybrid Cloud Security'yi tercih etmelisiniz?

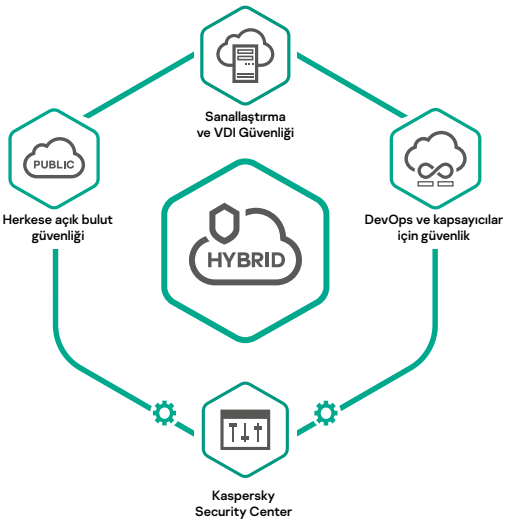
%30

geleneksel bir uç nokta güvenlik çözümü kullanmaya kıyasla sanallaştırma donanım kaynaklarında sağlanabilecek olası tasarruf oranı.

İLK 3

devamlı olağanüstü performans. Geçtiğimiz yıl Kaspersky ürünleri, birden fazla bağımsız testte bir kez daha olağanüstü standartlarda bir performans göstererek 57 birincilik elde etti ve 63 defa ilk üç arasında yer aldı (kaspersky.com.tr/top3 adresinden daha fazla bilgi edinebilirsiniz).

Tüm bulut gereksinimleriniz için bir ürün



Kapsayıcılar

Herkese açık bulut ortamları

Fiziksel ve Sanal Makineler

Tek Ürün | Tek Konsol | Tek Lisans

Müşteri görüşleri

"Bu çözüm, sistem performansını etkilemeden veya kullanıcı deneyimini kesintiye uğratmadan sanal ve bulut ortamlarının korunmasına yardımcı olur."

"Tüm güvenlik çözümlerini tek bir lisansta birleştirmek harika bir yöntem."

"Ekstra virüsten koruma yazılımı ve başka aracılar yüklemeye gerek kalmıyor."

"Veri koruması için merkezî bulut çözümü. Tek bir yerde."

"Yeni güncellemeler indirmeniz gerekmediği için koruma, tüm sanal makinelere anında uygulanır."

"Uzun süreli yönetici eğitimi gerektirmeyen ideal çözüm."

Amazon ve Gartner incelemelerinden alınmıştır

Bir demo talep edin

www.kaspersky.com.tr