Kaspersky® Hybrid Cloud Security

Hibrit Bulut Sisteminiz için Kanıtlanmış Koruma ve Sınırsız Düzenleme

Bulut teknolojisine geçiş yapanların karşılaştıkları başlıca zorluklar:

- Altyapı karmaşıklığının artması, şeffaflığın azalmasına neden olabilir
- Güvenilir korumanın en önemli yöntemi olan çok katmanlı yaklaşım, nadiren tek bir üründe görülür
- Geleneksel ağır güvenlik çözümleri, değerli sistem kaynaklarını tüketir
- Ayrık bir yaklaşım ve birbirinden tamamen farklı kontroller, ek yönetim ve güvenlik sorunlarına yol açar
- Sanal ve fiziksel uç noktalara, kötü amaçlı yazılım ve fidye yazılım saldırıları görülebilir
- Kişisel verilerin korunması için yeterli siber güvenlik önlemleri uygulayamamak, yasal sorunlara neden olabilir.

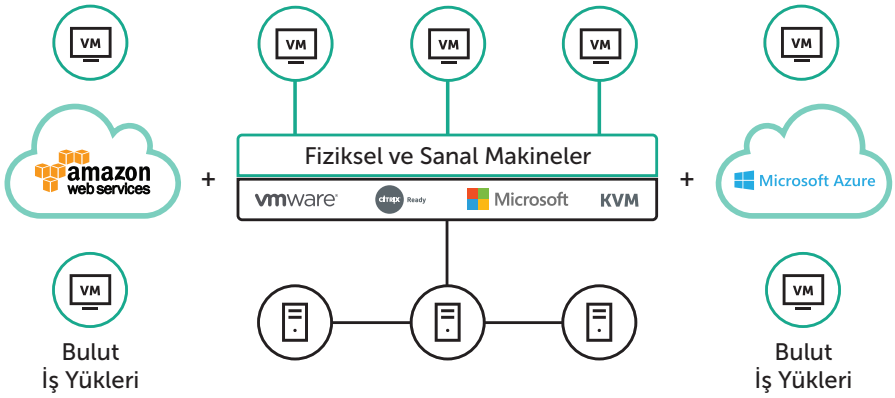
Neden Kaspersky Hybrid Cloud Security Çözümünü Seçmelisiniz?

- Fiziksel, sanal ve bulut iş yükleri için geliştirilmiştir
- Her türlü iş yükü türü için entegre ve çok katmanlı güvenlik
- AWS ve Azure gibi herkese açık bulutlar için sorunsuz, otomatik ve çevik güvenlik
- Güvenlik araçlarından oluşan eksiksiz bir set ile ortak sorumlukları yerine getirmeye yardımcı olur
- Hibrit bulutunuzun tamamında sorunsuz güvenlik düzenlemesi
- Birçok ödüle ve bağımsız teste göre en çok test edilen ve en güvenli koruma[1]
- Gartner Peer Insights Platinium Müşteri Ödeli dahil olmak üzere müşterilerin güvenini ve saygısını kazanan teknolojileri temel alır.

1 Burada bahsedilen testler, Kaspersky Hybrid Cloud Security çözümünde kullanılan tehditlere karşı koruma teknolojilerine dayalı çeşitli Kaspersky Lab ürünlerini kapsar.

Sanallaştırma, esnek ve etkili olmaya çalışan her işletme için temel yaklaşım haline gelmiştir. Bulut bilişim, doğal olarak bu yaklaşımı takip eden bir sonraki aşamadır. Karmaşık altyapı desteğinin kısıtlamalarını ortadan kaldırır ve daha önce ulaşılamayan bir verimlilik düzeyi sağlar. Ancak bulut bilişim yolculuğunun da riskleri ve sorunları vardır. Bu sorunların bazıları yeni ortaya çıkmışken bazıları ise fiziksel dünyadan kalan sorunlardır.

Kaspersky Hybrid Cloud Security, bulut bilişim yolculuğunuzun her aşamasında veya durumunda birleşik güvenlik sunar. Hem buluta geçiş hem de yerel bulut senaryoları için uygun olan bu çözüm şirket içinde, veri merkezinde veya herkese açık bulut ortamında çalışırken fiziksel ve sanal iş yüklerinizi korur. Çözümün içindeki uygulamalar hem sanallaştırmanın hem de sunucu işlevinin kendine özgü özellikleri düşünülerek geliştirilmiştir. Bu sayede, mevcut ve gelecekteki en gelişmiş tehditlere karşı son derece dengeli bir koruma sağlanırken sistem performansından taviz verilmez.



Temel Avantajlar

Buluta güvenli bir şekilde geçmenizi sağlar.
Koruma düzeyinden taviz vermenize gerek kalmaz.

- Patentli teknolojiler ve ödüllü siber güvenlik motorumuz fiziksel, sanal veya bulut tabanlı tüm iş yüklerinizi korur.
- Makine öğrenimi destekli çok katmanlı gerçek zamanlı koruma verilerinizi, süreçlerinizi ve uygulamalarınızı yeni ortaya çıkan tehditlere karşı korur.
- Veri güvenliği konusunda bütüncül bir yaklaşım benimsenmesi, veri koruma düzenlemeleriyle ilgili yasal riskleri ve itibar kayıplarını azaltmaya yardımcı olur.

Kaspersky Humachine™ Yaklaşımı

Büyük Veri tehdit istihbaratının, robotik makine öğrenimi becerilerinin ve uzman deneyiminin kusursuz birleşiminden güç alan Kaspersky HuMachine™, birçok avantaj sunar ve daha etkili bir koruma sağlar. Birbirinden ayrı bileşenler, her bir parçanın birbirine bağlanmasıyla daha etkili ve verimli bir bütün haline gelir.

Kaynaklarınızından ve yatırımlarınızdan en iyi şekilde yararlanmanızı sağlar

- Aracısız ve hafif aracılı koruma, performansı etkilemeden sanallaştırılmış varlıkları ve yazılım tanımlı ağları düzenli olarak korur.
- Yerel, herkese açık ve yönetilen bulut güvenliği ile entegrasyon yapılması; uygulamalarınızın, işletim sistemlerinin, veri akışlarının ve kullanıcı çalışma alanlarının güvenliğini sağlamanıza yardımcı olur. Tüm bunları, kaynaklarınızı mümkün olan en düşük seviyede kullanarak başarır.
- Fiziksel ve sanal kaynakların tek bakış açısıyla yönetimi, geçiş ve bakım sırasında çalışma saatlerinden tasarruf etmenizi sağlar.

Çözüm, hibrit altyapı yapılandırmanıza bakılmaksızın şeffaf görünürlük ve kontrol sağlar

- Yönetilebilirlik ve güvenlik düzenlemeleri, birden çok bulutta sorunsuz bir şekilde çalışır.
- Tam görünürlük, kontrol ve her konumda her iş yükü için en gelişmiş tehditlere karşı bütüncül koruma.
- Güvenlik hizmetleri daha kolay sağlanır ve ilke temelli işlemler, hibrit bulutunuzun tamamında etkinleştirilir.

Özellikler

HuMachine destekli, tehditlere karşı çok katmanlı koruma

Kaspersky'nin Yeni Nesil kötü amaçlı yazılımlara karşı koruma teknolojisi, işiniz açısından kritik iş yüklerinizi tehdit eden çok çeşitli siber saldırıları engelleme kapasitesine sahip birden çok proaktif güvenlik katmanı içerir.

- **Global tehdit istihbaratı**, tehdit ortamı değişirken bile bu ortamın durumuyla ilgili gerçek zamanlı veriler sağlar ve daima güvenliğinizi korur.
- **Makine Öğrenimi:** Global tehdit istihbaratından oluşan büyük veri, minimum sayıda hatalı pozitif sonuç veren başarısını kanıtlamış yüksek tespit düzeyi için makine öğrenimi algoritmalarının ve insan uzmanlığının birleşimi tarafından işlenir.
- **Web ve e-posta tehdit koruması,** sanal ve uzak masaüstlerinin güvenliğini sağlar ve bunları e-posta ve web temelli tehditlerden korur.
- **Dosya Bütünlüğünü İzleme,** kritik sistem bileşenlerinin ve diğer önemli dosyaların bütünlüğünü sağlamaya yardımcı olur.
- **Günlük Denetimi,** optimum düzeyde operasyonel hijyen için dahili günlük dosyaları tarar.
- **Davranış Analizi,** uygulamaları ve süreçleri dosyasız veya komut temelli kötü amaçlı yazılımlar dahil olmak üzere gelişmiş tehditlere karşı korur.
- **Düzeltme Motoru,** gerekli olduğu durumlarda bulut iş yüklerinde yapılan her türlü kötü amaçlı değişikliği geri alır.
- **Güvenlik Açıklarından Yararlanan Yazılımları Önleme,** saldırının öncülerine karşı etkili koruma sağlar ve korunan uygulamalara mükemmel şekilde uyum gösterir. Ayrıca tüm bunları yaparken performansa minimum düzeyde etki eder.
- **Fidye yazılımlarına karşı koruma işlevi,** iş açısından kritik verileri rehin tutma girişimlerine karşı sanal iş yüklerini korur, saldırıdan etkilenen dosyaları şifrelenmemiş durumlarına döndürür ve uzaktan başlatılan şifreleme girişimini engeller.

Tüm bulutlar için birleşik güvenlik

Herkese açık bulutlar
- Amazon Web Services (AWS)
- Microsoft Azure

Özel veri merkezleri
- Vmware NSX
- Microsoft Hyper-V
- Citrix XenServer
- KVM
- Proxmox

VDI ortamları
- Vmware Horizon
- Citrix XenDesktop

Fiziksel sunucular
- Windows
- Linux

- **Ağ Tehditleri Koruması,** bulut tabanlı varlıklara ağ temelli sızma girişimlerini tespit eder ve engeller.

Sistemi güçlendirmek, direnci artırır

- **Uygulama Kontrolü,** optimum düzeyde sistem güçlendirmesi için Varsayılan Olarak Reddet modunda tüm hibrit bulut iş yüklerinizi kilitlemenizi sağlar. Bu sayede çalışan uygulamaları yalnızca yasal ve güvenilir uygulamalarla sınırlayabilirsiniz.

- **Cihaz Kontrolü,** hangi sanallaştırılmış cihazların hangi bulut iş yüklerine erişim sağlayabileceğini belirler.

- **Web Kontrolü,** riskleri azaltmak ve üretkenliği artırmak için sanal ve uzak masaüstleri tarafından web kaynaklarının kullanımını düzenler.

- **Ana Bilgisayar Tabanlı İzinsiz Giriş Önleme Sistemi (HIPS),** başlatılan uygulamalar için güven kategorileri atar ve bu uygulamaların kritik kaynaklara erişimini ve bazı özelliklerini kısıtlar.

Sınırsız görünürlük

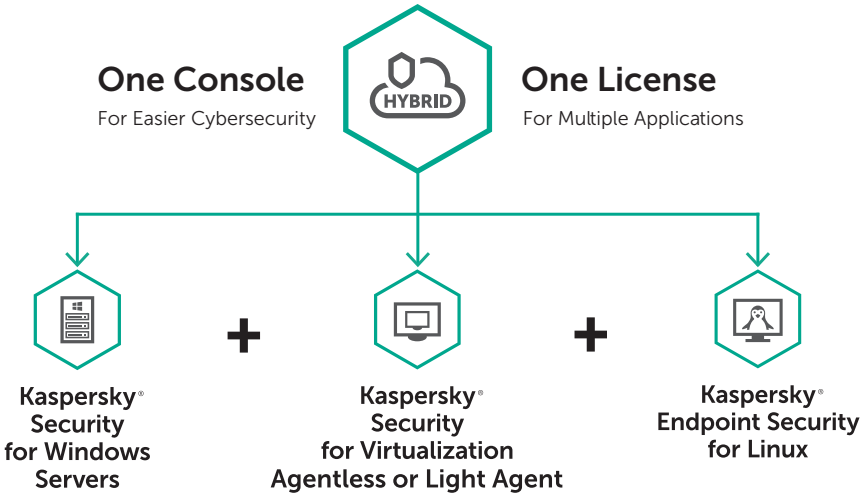
- **Birleşik Güvenlik Yönetimi,** Kaspersky Security Center tabanlıdır. Bu özellik ofisinizdeki, veri merkezinizdeki ve buluttaki tüm altyapıda, uç noktalarda ve sunucularda tek bakış açısıyla güvenlik yönetimini kolaylaştırır.

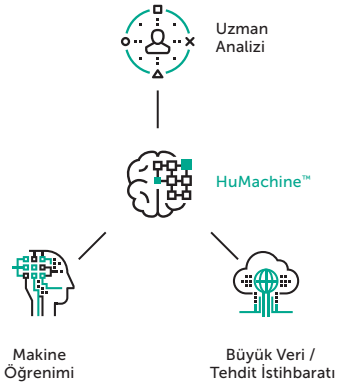
- **Bulut API:** Herkese açık AWS ve Azure ortamlar ile sorunsuz entegrasyon, daha kolay envanter ve güvenlik sağlamanın yanı sıra altyapının keşfini, otomatik güvenlik aracısı dağıtımını ve ilke temelli yönetimi kolaylaştırır.

- **Esnek yönetim seçenekleri,** çok kiracılı özelliğine, izin tabanlı hesap yönetimine ve rol tabanlı erişim kontrolüne olanak sağlar. Bu sayede esneklik sunarken tek bir sunucudan birleşik düzenlemenin avantajlarını korur.

- **SIEM Entegrasyonu:** Daha gelişmiş bir BT sistemine sahip altyapılarda Güvenlik Bilgileri ve Yönetim Sistemleri, tüm hibrit BT ağında şirketin siber güvenliğine farklı açılardan bakmak için birleşik bir pencere olarak kullanılabilir.

Kaspersky Hybrid Cloud Security, BT ortamı dönüşümünüzü desteklemek için çok sayıda ödüllü ve sektörde saygın güvenlik teknolojisi sunar. Çözüm, fiziksel ortamdan sanal ortama ve buluta geçişinizin güvenliğini sağlarken görünürlük ve şeffaflık özellikleriyle kusursuz bir güvenlik düzenlemesini garanti altına alır.





Kaspersky Lab
Enterprise Cybersecurity:**www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliği Haberleri:**business.kaspersky.com/**
Benzersiz yaklaşımım:**www.kaspersky.com.tr/true-cybersecurity**

#truecybersecurity
#HuMachine

www.kaspersky.com