KASPERSKY lab

Esnek hibrit bulut sisteminiz için geliştirilmiş sınırsız güvenlik

Kaspersky Hybrid Cloud Security

www.kaspersky.com
#truecybersecurity

Hibrit bulut ortamınız için geliştirilmiş sınırsız güvenlik

Veriler, her geçen gün daha akışkan hale gelmektedir. Sürekli olarak mobil cihazlarda kurumsal BT çevresinin dışında hareket eden veriler, aynı zamanda sanal ve fiziksel makinelerde de işlenir. Herkese açık bulutların ve yönetilen altyapıların ortaya çıkmasıyla veriler, şirket dışına daha önce görülmeyen bir düzeyde çıkmaktadır.

Kişisel veri merkezi kaynaklarının talep üzerine anında genişletilebildiği ve ihtiyaç duyulduğunda harici bulutlara aktarılabildiği esnek bulut hizmetleri modelinin gittikçe daha fazla şirket tarafından benimsenmesi, emsalsiz bir esneklik, çeviklik ve belirgin ekonomik avantajlar sağlar. Bu modelde altyapıya önceden yatırım yapılması gerekli değildir, kaynaklar boşa kullanılmaz ve kaynak sağlama gereksinimleri anında karşılanabilir. Ayrıca tüm bunların yanı sıra yönetilebilirlik sürdürülür.

Herkese açık bulutlar, başka bir avantaj daha sağlar. Bu avantaj iş sürekliliğidir. Veri merkezinizde kesinti veya hasar sorunu yaşıyorsanız sorun düzelene kadar şirket dışı kaynakları kullanarak işinizi devam ettirebilirsiniz. Herkese açık bulut hizmeti sağlayıcıları, kendi iş sürekliliklerine ve siber güvenliklerine ciddi yatırımlar yaparak iş yükleriniz için güvenli ve dirençli ortamlar oluşturur. Ancak konunun başka bir tarafı daha vardır...

Bulut kullanıcıları için Başlıca Güvenlik Sorunları

- Fiziksel, sanal ve bulut tabanlı iş yüklerine saldırdıran kötü amaçlı yazılımlar ve fidye yazılımları
- Reaktif ve organize olmayan güvenlik yaklaşımının sonucunda gerçekleşen veri sızıntıları
- Artan altyapı karmaşıklığı nedeniyle azalan şeffaflık
- Birbirinden ayrı kontroller ve araçlar nedeniyle yaşanan yönetim zorlukları
- Ağır geleneksel çözümlerle boş yere harcanan sistem kaynakları.
- Özel veri merkezleri içinde depolanan veriler için yetersiz koruma
- Operasyonel süreklilği veya veri değişimini engelleyen DDoS saldırıları

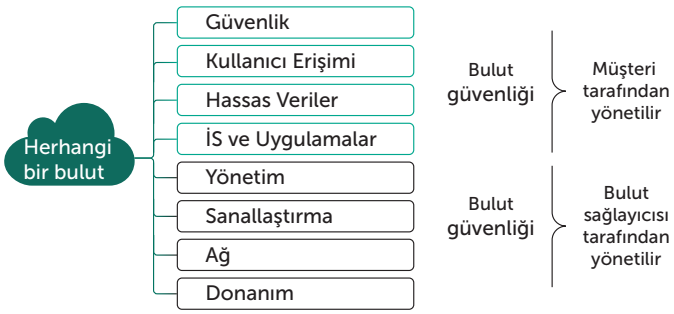
Verileriniz herkese açık bulutlarda ne kadar güvendedir?

Bu sorunun cevabı göründüğü kadar basit değildir.

Herkese açık bulutlar, şu andaki durumlarıyla son derece güvenli yerlerdir. Sağlayıcılar, verilerinizin kesinlikle barındırılan ortamda kalmasını ve bulut içinde veya harici bulutun ötesinde sızıntı riskinin ortadan kalkmasını sağlamak için daima büyük bir özen gösterir.

Ancak verilerin güvenli bir şekilde kontrol altında tutuluyor olması, her zaman güvende oldukları anlamına gelmez. Veri sızıntısı, güvenliğin yalnızca bir yönüdür. Örneğin fidye yazılımlarına maruz kalan veriler eksiksiz ve güvenli bir şekilde saklanıyor olmasına rağmen zarar görebilir ve bu nedenle tamamen kullanılamaz

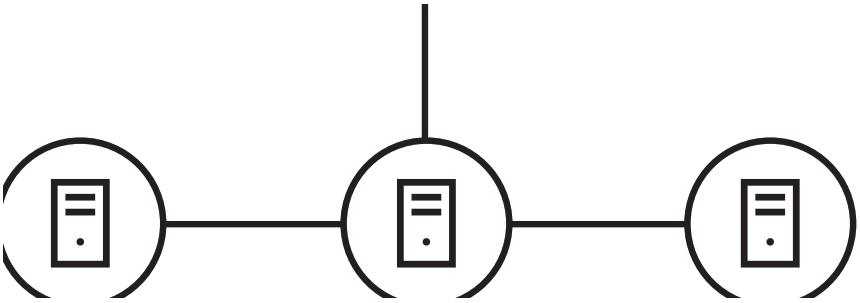
Paylaşımlı Güvenlik Sorumluluğu Modeli



hale gelebilir. Ayrıca insanlarla etkileşime giren her türlü veri, (kurumsal bir varlık olarak verilerin temel fonksiyonu zaten budur) insan hatasının ve olası kötü niyetli kişilerin etkilerine maruz kalır.

Barındırılan bulut hizmeti sağlayıcıları, sundukları ortamın güvenliğini sağlamaktan sorumludur. Ancak iş yükü nerede bulunursa bulunsun her iş yükünün dahili güvenliğinin sorumluluğu size aittir. Bu durum "Ortak Güvenlik Sorumluluğu" modeli olarak bilinir. Bu modelde, siz ve hizmet sağlayıcınız iş ilişkinizin ve veri varlıklarınızın güvenliğiyle ilgili olarak farklı konulardan sorumlu olursunuz.

Bu nedenle "Verileriniz herkese açık bulutlarda ne kadar güvendedir?" sorusunun cevabı en iyi ihtimalle şudur: "Verileriniz, herhangi bir yerde olduğu kadar güvendedir." Nereye aktarılırsa aktarılsın veriler için aynı güvenlik sorunları geçerlidir. Verilerinizin herhangi bir zaman dilimi içinde bulunduğu yerin güvenliğini sağlamak, verilerinizi korumak için yeterli değildir. Kurumsal BT çevresinin kontrollü ortamının dışına aktarılan iş açısından kritik verilerin hacmi, her geçen gün arttığı için bu gerçeği kavramak büyük önem taşır.



Yalnızca çevresindekileri değil verilerinizi de koruyun

Veri paketi aktarım halindeyken veya herhangi bir yerde depolanırken dahili olarak korunmalıdır. Bu, şirketinizin sorumluluğundadır. Bu sorumluluk için dış kaynak kullanılamaz veya başkasına yetki verilemez.

İş akışınızın güvenliğini sağlamak için bunu düzenleyebilmeniz gereklidir

O halde öncelikle şu soruyu sormalıyız: Her bir veri paketinizin herhangi bir zamanda nerede olduğunu veya nereye doğru hareket ettiğini ve kiminle etkileşime girdiğini tam olarak biliyor musunuz?

Erişim kontrolü ve izleme, süreklilik gerektiren bir güvenlik meselesidir. BT altyapınız daha geniş ve karmaşık hale geldikçe verimliliği ve sistem performansını optimize etmek için daha çok çözüm gerekir ve her bir iş yükü ve uygulamanın izini sürmek zorlaşır. Harici kaynakları barındırmak için veri merkezi altyapılarının genişlemesi, bu soruna başka bir boyut getirir. Şirket içinde ve dışında hangi verilere erişim sağlandığını ve hangi verilerin işlendiğini ve bunun nasıl gerçekleştiğini tam olarak belirleyebilmek büyük önem taşır.

İş yüklerinizin güvenliğini sağlamak için onları güçlendirebilmeniz gereklidir

Neler oluyor? Hangi uygulamalar nerede çalışıyor ve her uygulama gerektiği gibi çalışıyor mu? Uygulamalardaki güvenlik açıkları, sızma ve bulaşma saldırıları için siber suçluların kullandığı temel yöntemdir. Sistem güçlendirmesi, bunun olmasını engellemek için teknoloji katmanları kullanılarak gerçekleştirilir. Belirli uygulamaları yasaklamak veya kısıtlamaktan kuruluşunuzda çalışan her uygulamanın davranışlarını izlemeye ve güvenlik açıklarından yararlanılmaması için koruma sağlamaya kadar tüm kritik tehdit önleme ve tespit kontrolleri ve müdahaleleri sizin sorumluluğunuzdadır.

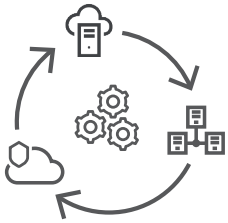
Kuruluşunuzun güvenliğini sağlamak için verilerinizi koruyabilmelisiniz

Runtime verilerinizi koruyabilmeniz için bu verilerin ne zaman ve ne tarafından olası veya gerçek bir saldırıyla karşı karşıya olduğunu anlayabilmeniz gereklidir. Verileriniz, özellikle işletmenizi hedef alan APT'lerden (Gelişmiş Sürekli Tehdit) fırsatçı fidye yazılımlarına; veri hırsızlığı ve finansal dolandırıcılıktan insan hatasına kadar her türlü tehditle karşı karşıya gelir. Siber suç son derece karlı ve gelişmiş bir sektör olduğu için sürekli olarak yeni saldırı yöntemleri geliştirilmekte ve uygulanmaktadır.

Buluttaki veriler için geçerli olan kurallar tüm veriler için geçerlidir. Güvenlik sisteminizin dayalı olduğu tehdit istihbaratının kalitesi ve bu istihbaratın zamanında ve doğru şekilde uygulanması mevcut korumanızın etkililiğini belirler. Olası bir tehdit verilerinize ulaşmadan ve çalışmalarınızı etkilemeden önce BT güvenlik sisteminiz, bu tehdidi belirleyebilmeli, engelleyebilmeli ve düzeltebilmelidir. Ayrıca bu işlemleri sistem performansınızı etkilemeden ve en önemlisi kesintilere neden olan ve kaynaklarınızı yanlış alarmlarla tüketen "hatalı pozitif sonuçlar" üretmeden gerçekleştirebilmesi gerekir.

Bu önlemlerin tamamı da sizin sorumluluğunuzdadır. Bulut hizmetleri sağlayıcınız, verilerinizi yalnızca belli bir noktaya kadar koruyabilir; gerisi size aittir.

Hibrit bulut veri merkezinizin güvenliğini sağlarken nelere dikkat etmelisiniz



Özet olarak iş yüklerinizi çalıştırabileceğiniz güvenli ve tamamen sınırlı bir ortam sunması için harici veri barındırma yazılımı sağlayıcılarına başvurabilirsiniz. Ancak verileriniz nerede olursa olsun her bir parçasını izlemek, kontrol etmek ve korumak sizin sorumluluğunuzdadır.

Kaspersky Lab olarak Siber Güvenlik Düzenlemesi, Sistem Güçlendirmesi ve Runtime Koruması olmak üzere güvenlik sorumluluğunun üç alanını üstleniriz. Bu güvenlik katmanlarından her birini, aşağıda gösterildiği üzere belirli tamamlayıcı ve birbirine bağlı
teknolojiler aracılığıyla uygularız.

Hibrit bulut ortamınızı korumak için bir çözüm seçerken aşağıdakiler başta olmak üzere bazı gereklilikleri belirtmenizi öneririz:

Sınırsız Düzenleme

Bulut API: Yerel API aracılığıyla herkese açık bulutlarla (Amazon AWS ve Microsoft Azure gibi) entegrasyon. Bu özellik altyapı keşfi, otomatik güvenlik aracılarının dağıtımı ve ilke tabanlı yönetim sağlar.

Hesap Yönetimi: Bulut tabanlı makineleri kilitlemenin yanı sıra güvenlik operatörlerinin ve yöneticilerinin siber güvenlik konsolunun belirli alanlarına erişmesi için doğru izinlere sahip olmasını sağlayarak operasyonel hijyeni artırma

Rol Tabanlı Erişim Kontrolü: Altyapı ve güvenlik ekipleriniz, onlara atadığınız operasyonel görevlere bağlı olarak hibrit bulut ortamınızın siber güvenlik katmanlarında farklı erişim ve kontrol düzeylerine sahip olabilir.

Sistem Güçlendirme

Uygulama Kontrolü ve Beyaz Listeye Alma: Hangi uygulamaların nerede ve ne zaman çalışacağını belirlemek veya kontrol etmek, saldırı yüzeyinizi küçültür (Kaspersky Lab, her müşterimiz için hangi uygulamaların güvenli bir şekilde çalışabileceğini belirleyen kendi Beyaz Listeye Alma Laboratuvarı'na sahip olma konusunda benzersizdir. Bu özelliği sayesinde gerektiğinde son derece güvenilir bir "varsayılan olarak reddet" ilkesi uygulayabilir)

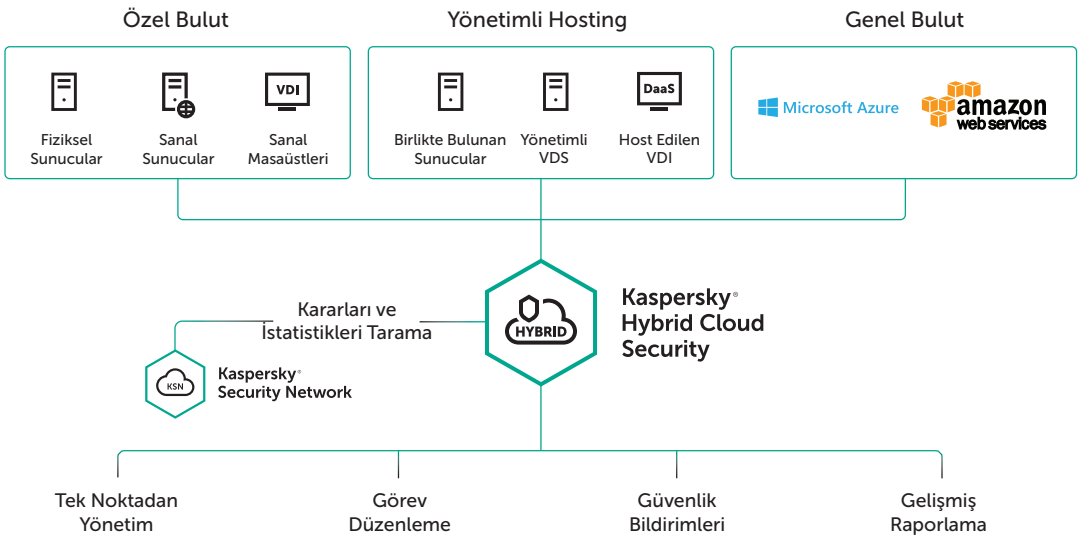
Güvenlik Açıklarına Karşı Koruma: Kullanıcılarınızın tercih ettiği popüler uygulamalardaki güvenlik açıkları aracılığıyla saldırganların sistemlerinize sızmasını önleyen güvenlik açığı önleme, güvenlik açığı tespiti ve otomatik güvenlik eki yönetimi (tabii ki bu işlevlerin hepsi Kaspersky Security for Hybrid Clouds'a dahildir) gibi teknikler.

Runtime Koruması

Fidye yazılımlarına karşı koruma: E-posta ve web kötü amaçlı yazılımları dahil olmak üzere fidye yazılımı sızıntısını önleme. Ayrıca Kaspersky Security for Hybrid Clouds, "otomatik geri alma" özelliğine sahiptir. Bu sayede bozulan dosyalar, otomatik olarak eski ve şifrelenmemiş durumlarına döndürülür.

Gelişmiş Tehdit İstihbaratı: sistemleriniz ve veri koruma mekanizmalarınız için yüksek kaliteli ve gerçek zamanlı tehdit istihbaratına erişim ve bu istihbaratı uygulayabilme.

Bu son özellik en kritik unsurdur. Bu özellikte yapay zeka ön plana çıkmaktadır. Bir sistemin, daha önce hiç karşılaşmadığı tehditleri tanımak ve tanımlamak için yazılım veya davranış anormalliklerini belirleme becerisinden yararlanılır. Bu, doğrudan bulut tabanlı istihbarat veri merkezlerinden istihbarat almak ve uzmanların müdahaleleri aracılığıyla makine öğrenimi ve davranışsal analiz dahil olmak üzere çeşitli tekniklerden oluşan bir birleşimin kullanılmasıyla başarılır.



Bilinmeyen tehditleri tanımlayabilme ve bunlara karşı koruma sağlama veri güvenliğinin vazgeçilmez unsurlarındandır. "'HuMachine® intelligence" (uzmanların ve uzman sistemlerin birlikte çalışması) olarak adlandırdığımız bu düzey olmadan ne kadar çok güvenlik teknolojisi kullanırsanız kullanın verileriniz gelecekteki saldırılara açık hale gelir. Kaspersky Lab çözümleri, bu makine istihbaratının (teknolojilerimizde makine öğrenimini on yıldan daha uzun bir süredir kullanıyoruz) ve rakipsiz uzmanlığın birleşimini temel alır. Bu sayede günümüzün ve geleceğin tehditlerini tespit edebilir, tanımlayabilir ve engelleyebiliriz.

Gerekliği olduğu kadar gelişmiş bulut güvenliği

Kaspersky Lab'in Hibrit Bulut Güvenliği çözümü, yukarıdaki gerekliliklerin tamamını ve daha fazlasını sunar. Bu çözüm, hibrit bulutunuzun tamamını en gelişmiş tehditlere karşı korumak için uyarlanabilir bir güvenlik ortamı sunar.

Esnek ve Güvenli Bulutlar

Hibrit ortamlar son derece dinamiktir. Güvenlik yaklaşımınız, değişen operasyonel durumunuz gelişirken ve ölçeklenirken hızlıca uyarlanabilmelidir.

- Üstün uçtan uca koruma için bulut ortamlarında görünürlüğü hızlandırın.
- İnsanların ve makinelerin ortak gücünden faydalanarak gelişmiş siber tehditleri tespit edin ve yanıtlayın.
- Bulut iş yüklerini, sistemleri, ağları veya verileri birden çok kontrolle koruyun.

Tüm Bulutlarda Kullanılabilen Tek Bir Ürün

Kurumsal düzeydeki hibrit bulut ortamlarına yönelik yeni nesil siber güvenlik hizmetleri sunmak için geliştirilen bir çözüm.

- Fiziksel ve sanal sunucular, VDI, depolama ve hatta özel bulutunuzdaki veri kanalları için başarısını kanıtlamış güvenlik.
- AWS ve Azure dahil olmak üzere herkese açık bulutlardaki iş yükleri için gelişmiş güvenlik kontrolleri.
- Siber riski en aza indirerek kurumsal Hizmet Düzeyi Hedefleri'ni (SLO) karşılar.

Kusursuz Güvenlik Deneyimi

BT ve Güvenlik sisteminizin şeffaflığı ve çapraz entegrasyonu bilinen, bilinmeyen ve gelişmekte olan tehditlere karşı güvenlik durumunuzu belirler.

- Yerel API aracılığıyla bulutunuzun temel teknolojileri ve güvenlik katmanınız arasında entegrasyon
- Güvenli ve risksiz bulut geçişi için otomatik güvenlik sağlama
- Her bulut için kurumsal düzeyde sorunsuz güvenlik düzenlemesi deneyimi

Hibrit Bulut Güvenliği çözümümüzdeki gelişmiş özellikler sayesinde altyapı ve güvenlik katmanları entegre edilebilir ve birlikte çalışır. Bu çözüm, iş yüklerinin özel ve herkese açık bulutlar arasında sınırsız güvenlik geçişini sağlayacak güvenli ve etkili bir ortam oluşturmak amacıyla iki gücü birleştirir. Böylece sürekli, esnek, şeffaf ve yönetilebilir güvenlik elde edilir ve hibrit ortamları işlerinizin gerektirdiği kadar kullanabilirsiniz.

Özet olarak...

Dışarıdan yönetilen bulut tabanlı barındırma hizmetleri, işiniz için önemli avantajlar sunar ve kurumsal verilerin güvenli bir şekilde depolanabileceği ve işlenebileceği güvenli ortamlar sağlar. Ancak iş paketlerinizin güvenliğinin sorumluluğu size aittir. Verileriniz, süreçleriniz ve uygulamalarınız üzerinde tam görünürlüğü ve kontrolü hiç durmadan sürdürerek ve veri koruma yaklaşımınızda "HuMachine"® tabanlı gelişmiş tehdit istihbaratını uygulayarak hibrit bulut veri merkezinizin tüm güvenlik gereksinimlerini karşılayabilirsiniz.

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