Kaspersky® Hybrid Cloud Security

Microsoft Azure Cloud Varlığınızı Koruma

Günümüzde herkese açık ve yönetilen bulutlar, kurumsal BT ortamının bir parçası haline gelmiştir. Microsoft Azure gibi herkese açık bulutların iş açısından kritik yükleri bile kaldırabilecek kadar geliştiğinin anlaşılması ise yeni bir durumdur.

Bu yenilikler, kurumsal işletmelerin güvenlik vizyonunu ve BT stratejilerinin geliştirilmesini etkileyecektir. BT altyapınız önümüzdeki üç ila beş yıl içinde nasıl ölçeklendirilecek ve gelişecek? Herkese açık ve yönetilen bulutların özelliklerinden en iyi şekilde faydalanırken ortaya çıkan hibrit altyapının nasıl güvenilir ve güvenli olması sağlanacaktır?

Gittikçe daha fazla sayıda büyük kuruluş finansal ve hatta yasal sonuçların yanı sıra itibar kaybı gibi sorunlar yaşarken siber güvenlik olayları, herkes için endişe kaynağı olmaya devam etmektedir. Kurumsal güvenlik, mevcut ve gelecekteki tehditlere karşı mücadele edecek kadar çevik ve akıllı olmalıdır. Ayrıca hem herkese açık hem de özel bulut varlıklarını içeren hibrit bulut ortamınızla birlikte uyarlanabilecek ve gelişebilecek ölçeklenebilirliğe ve esnekliğe sahip olmalıdır.

Özel ve Genel Bulutlar: Hibrit Ortamınız

%51

İşletmelerin %51'i BT altyapısının karmaşıklığının uygun siber güvenlik düzeyleri elde etmelerini doğrudan etkilediğini kabul ediyor

Özel bulutunuzun güvenliğini sağlamak nispeten daha kolay bir iştir. Yazılım etkin bir veri merkezi oluşturmak için sanallaştırmanın kullanılması, daha yaygın bir uygulamadır. Kaspersky Lab, verimliliği optimize etmek ve sanallaştırma teknolojisinin sunduğu kaynak tasarrufu ve esneklik özelliklerini korumak amacıyla sanal makinede en hafif ayak izini bırakmak (veya VMware durumunda hiçbir fark edilebilir ayak izi bırakmamak) için özel yazılımlar sunmuş ve bu ihtiyacı karşılamıştır.

Ancak herkese açık bulut alanına geçiş yapmak ve özellikle hem özel hem de herkese açık bulutları aynı anda kullanmaya çalışmak ortaya yeni sorunlar çıkarmıştır. Güvenlik sorumluluğunuz nerede başlar ve biter, iş yükleriniz şirket içine ve dışına doğru hareket ederken bu yükleri nasıl düzenleyebilir ve koruyabilirsiniz?

Kullanmadan Önce Bilmeniz Gerekenler

%80'e varan oran

Hibrit bulutlardaki veri kaybının %80'e varan kısmı eski veya yeniden etkinleştiren siber güvenlik nedeniyle ortaya çıkıyor

Büyüklüğe, yazılım tanımlı özel veri merkezinde kullanılan sanallaştırma platformlarına veya iş açısından kritik uygulamaları yürütmek için seçilen bulut platformuna bakılmaksızın esnek bulut ortamlarında karşılaşılan bazı riskler vardır. Microsoft Azure gibi bulut hizmeti sağlayıcıları, herkese açık bulutların her ölçekteki bulut kullanıcısı için güvenli bir liman olmasını sağlamak amacıyla çok çaba gösterir. Azure, sınırsız kurumsal ortamlar oluşturmak için son derece verimli ve buluta özgü araçlar sağlar. Ancak bu önlemler, riski ortadan kaldırmaz.

Kaspersky Lab olarak buluta geçiş stratejilerinizi olumsuz olarak etkileyebilecek ve dijital dönüşüm sürecinizi yavaşlatabilecek çok ciddi tehditlerin (ve bu tehditler siber güvenlik alanıyla sınırlı değildir) olduğunu düşünüyoruz.

Veri İhlalleri veya Sızıntısı

Veri sızıntılarını önlemek için hibrit bulut ortamınızdaki her iş yükü için güvenilir siber savunma yöntemleri kullanmanızı öneririz. Ayrıca bunun için hem BT hem de güvenlik katmanlarının görünürlüğü ve şeffaflığı büyük önem taşır. Bu sayede korumanız gereken her iş yükünü görebilir ve hızla değişen esnek bulut ortamınızın her köşesine otomatik siber güvenlik özellikleri dağıtabilirsiniz.

Altyapı görünürlüğü günümüzün esnek dijital ortamları için önemli bir sorundur ve siber güvenliğinizin şeffaflığı azaldıkça hangi noktalarda ve ne zaman risk altında olduğunuzu tam olarak belirleyemeyebilirsiniz. Hatta bazen belirleyebilseniz bile çok geç kalmış olabilirsiniz. Bu parçalanmış güvenlik yaklaşımı, kurumsal hibrit bulutlarını siber suçlular açısından kullanışlı bir nokta haline getirir. Çünkü geleneksel ve bulut altyapılarına sızmak için genellikle aynı araçlar kullanılmaktadır. Ciddi bir veri ihlali; hassas müşteri veya iş ortağı bilgilerini, fikri mülkiyeti ve ticari sırları açığa çıkararak önemli sorunlara yol açabilir.

Veri Kaybı veya Veri Bütünlüğünün Bozulması

Veri bütünlüğünü korumanın en etkili yolu, makine öğrenimi destekli davranış analizi özelliğine sahip güçlü çalışma zamanı koruma fonksiyonları sunan siber güvenlik araçları kullanmaktır. Bu sayede en gelişmiş ve gizli tehditleri veya karmaşık fidye yazımlarını bile tanımlayabilirsiniz.

Veri ihlalleri genellikle kötü amaçlı etkinliğin bir sonucu olarak ortaya çıksa da verileriniz kötü amaçlı faaliyetlerin yanı sıra kendi son kullanıcılarınızın kasıtlı olmayan eylemlerinden dolayı erişilemez hale gelebilir veya zarar görebilir. Birçok kuruluş, mümkün olan en az RTO'yu (Kurtarma Süresi Hedefi) ve en kısa RPO'yu (Kurtarma Noktası Hedefi) sağlamak için veri kurtarma stratejileri geliştirir. Ancak verilerinizi yedeklemek veya kopyalamak, bu verileri geri döndürdüğünüzde bazı tatsız sürprizlerle karşılaşmayacağınız anlamına gelmez. Her türlü kuruma karşı başarılı ve son derece zararlı fidye yazılımı saldırıları sayısının hızla artması, veri bütünlüğünü korumanın oldukça zor bir iş olduğunu gösterir. Verileriniz ne kadar eski olursa olsun ve nerede bulunursa bulunur (fiziksel, sanal veya bulut iş yükü olarak) veri kaybı veya veri bütünlüğünün bozulması riski size aittir.

İstenmeyen veya Savunmasız Uygulamalar

En başarılı siber savunma stratejileri, uygulama başlatma denetimi (beyaz listeye alma, varsayılan olarak reddetme) ve güvenlik açıklarından yararlanan yazılımları engelleme özelliklerine dayalıdır.

Kurumsal son kullanıcılar birçok nedenle çok çeşitli sistemler ve uygulamalar yükler ve bunlarla çalışır. Son kullanıcıların cihazlarında veya iş açısından kritik sunucularda nelerin yüklü olduğunu her zaman kontrol edemeyebilirsiniz. Kurumsal ortam ne kadar geniş olursa her şeyi kontrol altında tutmak da o kadar zorlaşır. Tamamen güvendiğiniz iş açısından kritik uygulamalar bile sıfır gün açıklarına ve açıklardan yararlanan yazılımlara karşı tam anlamıyla dayanıklı olmayabilir ve olası siber risklere karşı anında düzeltme gerektirebilir.

Fazla Kaynak Tüketen Güvenlik Sistemleri

Hibrit bulutunuz ile kurucu bileşenlerinin tüm güvenlik unsurlarını net olarak anlamanın, en etkili koruma ve kaynak verimliliği birleşimini sağlayacak siber güvenlik özelliklerini uygulamanın sizin sorumluluğunuzda olduğunu bilmeniz önemlidir.

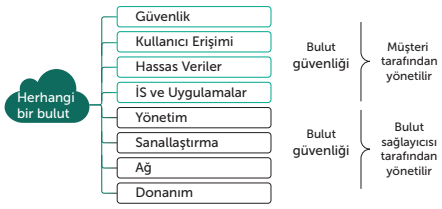
Hibrit bulutların çoğu, yazılım tanımlı veri merkezlerinin ve esnek herkese açık bulut hizmetlerinin bir karışımını kullanır. Her ikisi de koruma gerektirir ve farklı entegrasyon özellikleri sunan teknolojileri birleştirir. Hibrit bulut güvenliği için eski moda "her yerde geleneksel antivirüs" yaklaşımının benimsenmesi; bulut çözümlerinizin son derece verimsiz şekilde kullanımına, iş açısından kritik sistemlerin verimliliğinin risk altına girmesine ve dijital dönüşüm konusunda yatırım getirinizin önemli ölçüde azalmasına yol açabilir.

Güvenlik ve Altyapının Yanlış Ayarlanması

Herkese açık bulut API'ları ve uzantıları ile çalışmak, BT ve Güvenlik katmanları arasında güvenilir bir bağlantının kurulmasını sağlar. Böylece her ikisi de hibrit bulut ortamınızın büyüklüğüne bakılmaksızın birbirlerinin özelliklerinden faydalanarak ve güvenlik sağlamayı kolaylaştırarak birlikte çalışabilir.

Hibrit bulut teknolojisinin benimsenmesi, yeni bir dinamizm ve etkili envanter yönetimi gerektirir. Ayrıca yeni geliştirilen yüzlerce bulut iş yükü için sürekli olarak siber güvenlik sağlamayı zorunlu kılar. Bu durum, hiç bitmeyen bir BT güvenliği kabusuna dönüşebilir. Bir güvenlik uzmanı olarak BT alanındaki meslektaşlarınızın sürekli çoğalttığı bulut makineleri için kısıtlı veya gecikmiş görünürlük elde edebilirsiniz. Bu nedenle söz konusu makineler kurumsal ağı yeniden tarayana kadar savunmasız kalır. Ancak kıdemli BT personeli tarafından ağ segmentasyonu, yalıtım ve topolojinin yeniden yapılandırılması gibi yönetim görevleri için kullanılan araçlar ortaya çıkan siber tehditlere hızla yanıt verme ve uygun bir durum tespiti gerçekleştirme konusunda son derece kullanışlı olabilir. BT ve Güvenlik katmanlarınız arasında herhangi bir etkileşim yoksa güvenlik ekipleriniz göremedikleri şeyleri koruyamaz ve kıdemli BT personeliniz hibrit bulutunuzun tamamında gerçekten güvenli ve uyarlanabilir bir ekosistem oluşturmak için güvenlik ekiplerine yardımcı olamaz.

Genel Bulutlarda Ortak Sorumluluk



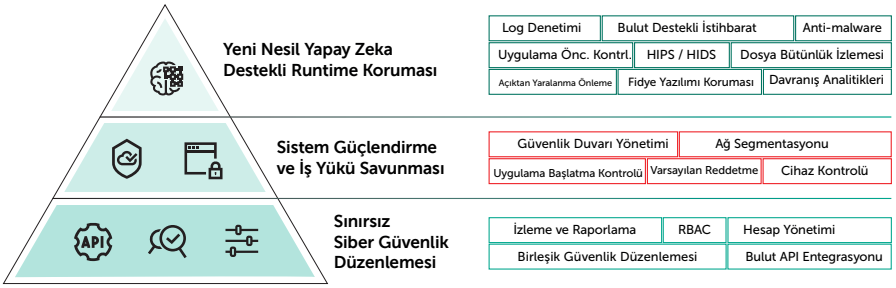
Herkese açık bulutlar kendi yerleşik güvenlik sistemlerine sahiptir. Ancak Ortak Sorumluluk Modeli, herkese açık bulutlardaki iş yüklerinizin, uygulamalarınızın ve verilerinizin güvenliğinin sizin sorumluluğunuzda olmasını zorunlu kılar. Bu iş yükleri iş açısından kritik öneme sahip olduğunda bu sorumluluk daha da önemli hale gelir. Microsoft Azure, olağanüstü güvenilirlik ve ölçeklenebilirlik özelliklerine sahip son derece gelişmiş bir bulut ortamı sunan lider bir herkese açık bulut hizmetidir.

Ancak ortak güvenlik sorumluluğu, herkese açık ve özel bulut ortamınızı kapsayan ve Azure tabanlı iş yüklerinizdeki verileri tam anlamıyla koruyan esnek bir siber güvenlik katmanı gibi ek özellikler gerektirir. Risklerin yanı sıra herkese açık ve özel bulut varlığınız dahil olmak üzere bulut ekosisteminizde bu tür riskleri nasıl çözebileceğinizi bilmeniz gereklidir.

Gerçek Yeni Nesil Koruma

Aşağıdakiler dahil olmak üzere proaktif yapay zeka destekli sistemler ve çalışma zamanı koruması ile Azure'un kendi buluta özgü araçlarını destekliyoruz:

- **Kötü amaçlı yazılımlara karşı ödüllü koruma motorumuz**, erişim veya talep üzerine her bulut iş yükü için otomatik ve gerçek zamanlı olarak dosya düzeyinde koruma sağlar.
- **Bulut destekli istihbarat,** yeni tehditleri hızlı bir şekilde tanımlar ve otomatik güncellemeler sağlar.
- **Davranış Tespiti,** uygulamaları ve süreçleri izler, gelişmiş tehditlere ve dosyasız kötü amaçlı yazılımlara karşı koruma sağlar ve gerektiğinde bulut iş yüklerinde yapılan kötü amaçlı değişiklikleri geri alır.
- **Güvenlik Açıklarından Yararlanan Yazılımlara Karşı Koruma,** sistem çalışma süreçlerini ve uygulama davranışlarını kontrol ederek fidye yazılımları dahil olmak üzere gelişmiş tehditleri engellemeye yardımcı olur.
- **Fidye Yazılımlarına Karşı Koruma,** bulut iş yüklerini ve paylaşımlı ağlarını saldırılara karşı korur ve saldırıdan etkilenen dosyaları şifrelenmemiş durumlarına geri döndürür.
- **HIPS / HIDS,** bulut tabanlı varlıklara ağ tabanlı sızma girişimlerini tespit eder ve önler.
- **Uygulama Kontrolleri,** optimum düzeyde sistem güçlendirmesi için Varsayılan Olarak Reddet modunda hibrit bulut iş yüklerinizi kilitlemenizi sağlar ve hangi uygulamaların nerede çalışabileceğini ve nelere erişim sağlayabileceğini belirler.
- **Cihaz Kontrolü,** hangi sanallaştırılmış cihazların hangi bulut iş yüküne erişim sağlayabileceğini belirler. Web Kontrolü ise internet tabanlı siber tehditlere karşı koruma sağlar.
- **Ağ Segmentasyonu,** hibrit bulut altyapı ağları için görünürlük ve otomatik koruma sağlar.
- **Güvenlik Açıklarına Karşı Koruma,** gelişmiş kötü amaçlı yazılımların ve sıfır gün tehditlerinin güvenlik eki uygulanmamış açıklardan yararlanmasını engeller.
- **E-posta Güvenliği,** istenmeyen e-postalara karşı koruma dahil olmak üzere bulut iş yüklerinde e-posta trafiğini korur.
- **Web Güvenliği,** Kimlik Avı Saldırılarına Karşı Koruma dahil olmak üzere tehlikeli web sitelerinden ve komut dosyalarından gelebilecek tehditlere karşı koruma sağlar.
- **Dosya Bütünlüğünü İzleme,** kritik dosyaları ve sistem dosyalarını korur. Günlük Denetimi ise operasyonel siber hijyen sağlamak için dahili günlük dosyalarını tarar.



Fiziksel sunucu ortamınızın yanı sıra sanal ve Azure bulut tabanlı kaynaklarınızı kapsayan tüm bu özellikler, birleştirilmiş bir güvenlik konsolu aracılığıyla tek bir Kaspersky Lab ürününde sunulur.

Azure Cloud'u Korumak için Siber Güvenlik Uzantıları

Kaspersky Lab yaklaşımı, Microsoft Azure Eklentileri ile birlikte çalışmayı içerir. Bu amaçla yalnızca bulut iş yükleriniz için yeni nesil yapay zeka destekli koruma uygulanmaz aynı zamanda doğrudan ve hatasız güvenlik izleme ve sağlama etkinleştirilir. Bu yönetim kolaylığı ve basitliği, Azure varlığınızda yürütülen iş yüklerinizin saniyeler içinde koruma altına alınması anlamına gelir. Böylece bulut tabanlı varlıklarınızı ve kullanıcılarınızı tam anlamıyla koruyabilirsiniz.

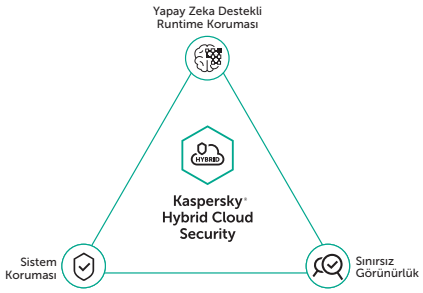
Öncelikle lider "yeni nesil" özelliklerimizi uygularız. Bu özellikler, günümüzde sektörde en çok test edilen, en çok ödül alan ve[1] en çok takdir edilen[2] koruma motorumuzu temel alır. Yeni nesil siber güvenlik, esnek ve uyarlanabilir bir bulut güvenliği ortamı geliştirmek için insanların ve makinelerin beraber çalışması anlamına gelir. Sizin ve entegre bulut tabanlı güvenliğinizin en gelişmiş siber tehditleri bile tespit etmesine ve bunlara yanıt vermesine yardımcı oluruz.

1 https://www.kaspersky.com/top3

2 Gartner Peer Insights Customer Choice Awards for Endpoint Protection Platforms

Neden Kaspersky Hybrid Cloud Security Çözümünü Seçmelisiniz?

- Fiziksel, sanal ve bulut iş yükleri için geliştirildi
- Her türlü özel veri merkezi için çok katmanlı entegre güvenlik
- Azure 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 kurumsal güvenlik düzenlemesi



Entegre Koruma, Görünürlük ve Düzenleme

Uçtan Uca Güvenlik

Herkese açık ve özel bulut altyapınızın tamamında bu çok katmanlı güvenlik kalitesini ve kapsamını uygulayarak hangi konumda olursa olsun her iş yükünün tamamen güvenli bir "uçtan uca" hibrit bulut ekosisteminde çalıştığını bilmenin rahatlığını yaşayabilirsiniz.

Buluta Uygun Güvenlik Sağlama

Azure Uzantıları sayesinde, tüm bu siber güvenlik özelliklerini bulut iş yüklerinizin içine yerleştirerek her zaman açık olan iş uygulamalarınızın güvende ve emniyette olmasını sağlayabilirsiniz.

Uyumluluk

Entegre güvenlik yaklaşımımız sayesinde Azure bulutunuza yüklediğiniz her şeyin güvenliğinin şirket standartlarınıza uygun olduğundan ve varlıklarınızın ve kullanıcılarının daima korunduğundan emin olabilirsiniz.

Birleşik Düzenleme

Azure Security Center ile entegrasyon sayesinde siber güvenlik bulut ekosisteminizin doğal bir parçası haline gelir.

Güvenlik Sağlamayı Kolaylaştırır

Doğrudan Azure MarketPlace'i kullanarak Azure iş yüklerinize gerçek zamanlı ve çok katmanlı koruma özelliklerini dağıtabilirsiniz.

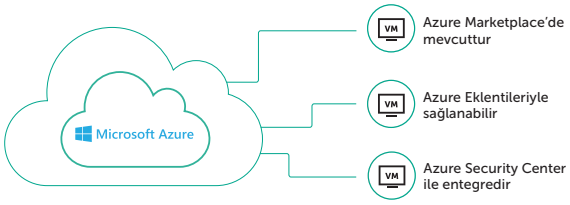
Esnek Lisans Seçenekleri

BYOL (Kendi Lisansını Getir) ve PPU (Kullanım Temelli Ödeme) dahil olmak üzere birden çok lisans ve fiyatlandırma seçeneği, BT ve dijital dönüşüm yatırımlarınızı optimize etmenize ve buluta geçme projenizde yüksek yatırım getirinizi korumanıza yardımcı olur.

İşe Yarayan Bulut Güvenliği

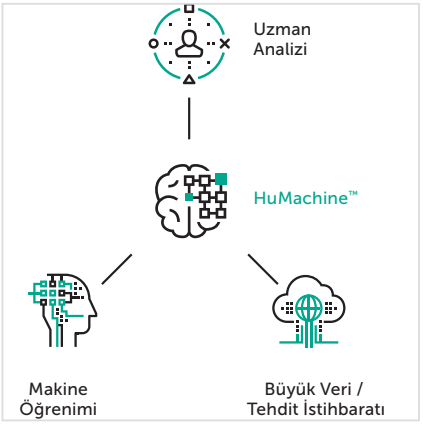
Sonuç olarak hibrit bulut iş yüklerinizin ihtiyaç duyduğu özellikleri tam anlamıyla sunan mükemmel şekilde düzenlenmiş ve uyarlanabilir bir siber güvenlik ekosistemi elde edebilirsiniz. Ayrıca kaynak verimliliği ve kusursuz düzenleme gibi avantajları koruyabilirsiniz.

Microsoft Azure



Kurumsal BT'nin Geleceğini Koruma

Microsoft Azure, kurumsal BT'yi değiştirmeye yardımcı olur. Kaspersky Lab olarak şu anda ve gelecekte hem Azure bulut varlığınızdaki hem de özel bulut ortamınızdaki tüm iş yüklerinizin güvenliğini, görünürlüğünü ve yönetilebilirliğini sağlamaya yardımcı oluruz.



Kaspersky Lab
Kurumsal Güvenlik: **www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenlik Haberleri: **business.kaspersky.com**
Benzersiz yaklaşımımız: **www.kaspersky.com.tr/true-cybersecurity**

#truecybersecurity
#HuMachine

www.kaspersky.com