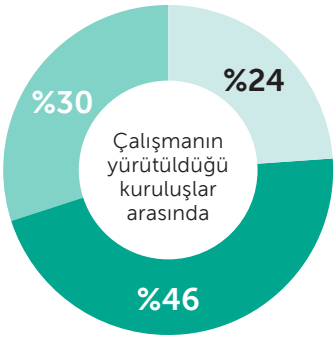
Kaspersky® Hybrid Cloud Security

Kurumsal Amazon Web Services Bulutunuzu Koruma

Günümüzde herkese açık ve yönetilen bulutlar, kurumsal BT ortamının bir parçası haline gelmiştir. Amazon Web Services (AWS) 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 altyapısı 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.



- Bulut kullanıp henüz denetim veya uyumluluk kontrolü yapmayanlar
- Bulut kullanıp oturmuş bir tehdit azaltma planı olmayanlar
- Bulut teknolojilerine, tamamen test edilmiş tehdit azaltma planıyla geçiş yapmış olanlar

Kaynak: Maintaining Control and Data Security in the Cloud report, Kaspersky Lab, 2017

Özel ve Herkese Açık Bulutlar: Hibrit Ortamınız

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

Güvenlik Tehditleri ve Riskleri Azaltma

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. Amazon gibi bulut hizmeti sağlayıcıları, herkese açık bulutların her ölçekteki bulut kullanıcısı için güvenli bir liman olmasını sağlamak amacıyla çok çaba gösterir. AWS, sınırsız kurumsal ortamlar oluşturmak için son derece verimli ve buluta özgü araçlar sağlar. Ancak bu önlemler, riski ortadan kaldırmaz.

Kaspersky Lab olarak bulutu benimseme 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

Kaspersky Lab olarak 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 yürütülen 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 veya nerede bulunursa bulunsun (fiziksel, sanal veya bulut iş yükü olarak) veri kaybı veya veri bütünlüğünün bozulması riski size aittir.

İstenmeyen veya Savunmasız Uygulamalar

Kaspersky Lab, bu sorunla nasıl mücadele edileceğini çok iyi bilir. 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 bulutunuzun ve kurucu bileşenlerinin tüm güvenlik unsurlarını net olarak anlamanın ve 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

Kaspersky Hybrid Cloud Security, API aracılığıyla BT ve bulut varlığınızın Güvenlik katmanları arasında güvenilir bir bağlantının kurulmasını sağlayan yerel entegrasyon özelliğine sahiptir. Böylece her ikisi de birbirlerinin özelliklerinden faydalanarak birlikte çalışabilir. Bu özellikler, hibrit bulut ortamınızın büyüklüğüne bakılmaksızın otomatik altyapı keşfi ve güvenlik sağlamayı içerir.

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 tamamından gerçekten güvenli ve uyarlanabilir bir ekosistem oluşturmak için güvenlik ekiplerine yardımcı olamaz.

Neden Kaspersky Hybrid Cloud Security Çözümünü Seçmelisiniz?

1. Fiziksel, sanal ve bulut iş yükleri için geliştirildi
2. Her türlü özel veri merkezi için çok katmanlı entegre güvenlik
3. AWS ve Azure herkese açık bulut hizmetleri için kusursuz, otomatik ve çevik güvenlik
4. Güvenlik araçlarından oluşan eksiksiz bir set ile ortak sorumlukları yerine getirmeye yardımcı olur
5. Hibrit bulutunuzun tamamında kurumsal güvenlik düzenlemesi

Herkese Açık Bulutlarda Ortak Sorumluluk

Herkese açık bulutlar kendi yerleşik güvenlik sistemlerine sahiptir. Ancak Ortak Sorumluluk Modeli, herkese açık bulutlardaki iş yüklerinizin, uygulamalarınızın ve verilerinizin sizin sorumluluğunuzda olmasını zorunlu kılar. Bu iş yükleri iş açısından kritik öneme sahip olduğunda bu sorumluluk daha da önemli hale gelir.

AWS, piyasada en gelişmiş ortamı sunan, olağanüstü düzeyde güvenilirlik ve ölçeklenebilirlik sağlayan ve sınırsız kurumsal ortamlar için çeşitli buluta özgü güvenlik araçları sağlayan lider herkese açık bulut hizmeti sağlayıcısıdır.

Ancak ortak güvenlik sorumluluğu, herkese açık ve özel bulut ortamınızı kapsayan ve AWS varlığınızdaki verileri tam anlamıyla koruyan esnek bir siber güvenlik katmanı gibi ek özellikler gerektirir.

AWS Bulut için Entegre Güvenlik

Sınıfının en iyisi koruma, görünürlük ve yönetilebilirlik

Gelişmiş siber güvenlik özelliklerimizin API aracılığıyla AWS'nin özellikleriyle sıkı bir şekilde entegrasyonu:

- **Sistem Verimliliği**
  Bulut altyapı envanteri, daha doğrudan ulaşılabilir hale gelir. Aynı şekilde konumlarına bakılmaksızın AWS EC2 örnekleriniz için otomatik güvenlik sağlamak da kolaylaşır. Bu tür sistem verimlilikleri, zaman ve kaynaklar açısından kayda değer tasarruflar sağlayabilir.
- **Tam Görünürlük**
  Görünürlük hibrit bulut ortamlarında önemli bir sorun haline gelebilir. Sıkı entegrasyon bu sorunu da çözer. AWS API aracılığıyla entegrasyon, her noktayı görebilmenizi, bulutunuzun nasıl düzenlendiğini anlamanızı ve bulut iş yüklerinizin tamamını koruduğunuzdan emin olmanızı sağlar.
- **Sorunsuz Düzenleme**
  AWS API entegrasyonu şirket içindeki ve buluttaki tüm BT varlıklarınızın tek bir konsol
  aracılığıyla birleşik yönetimine olanak tanır. Böylece tam şeffaflık, sorunsuz ve etkili düzenleme ve yönetim sağlanır.
- **"Bulut'tan" ve "Bulut İçin" Güvenlik**
  AWS EC2 örnekleriniz için sektörde lider korumamız, AWS MarketPlace'de de bulunabilir. Bu sayede buluta geçişiniz daha sorunsuz, kolay ve güvenli hale gelir. Bulut için en iyi güvenliğin bulutta mevcut olmasından daha iyi ne olabilir?
- **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 bir yatırım getirinizi korumanıza yardımcı olur.

Kaspersky Lab anlayışı, AWS ortamınız için sınıfında en iyi koruma, kaynak açısından verimli siber güvenlik ve kurumsal düzenleme özelliklerinden oluşan mükemmel şekilde dengelenmiş bir karışım geliştirmeyi hedefler. AWS API aracılığıyla kısmen entegrasyon sayesinde bu hedefi, herkesten daha iyi gerçekleştiriyoruz.

AWS ile birlikte çalışarak lider "Yeni Nesil" siber güvenlik özelliklerimizi uyguluyoruz. Bu özellikler, günümüzde sektörde en çok test edilen, en çok ödül alan[1] ve en çok takdir edilen[2] koruma motorunu temel alır. Yeni nesil siber güvenlik, esnek ve uyarlanabilir bir bulut güvenliği ortamı geliştirmek için insanların ve makinelerin beraber çalışması anlamına gelir. En gelişmiş siber tehditleri bile tespit etmenize ve bunlara yanıt vermenize yardımcı oluruz.

- **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 İstihbarat**, 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.

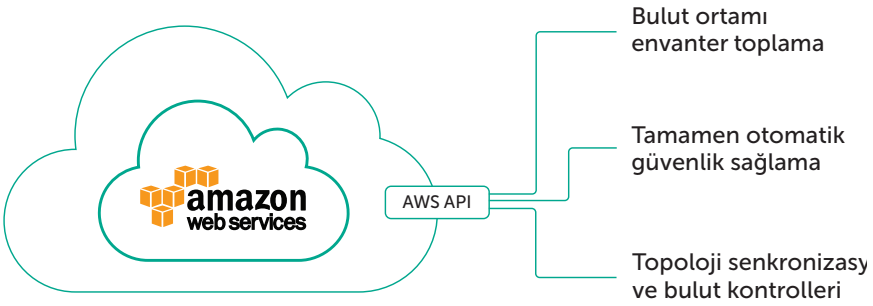
1 https://www.kaspersky.com/top3
2 Gartner Peer Insights Customer Choice Awards for Endpoint Protection Platforms

- **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 AWS bulut tabanlı kaynaklarınızı kapsayan tüm bu özellikler, birleştirilmiş bir güvenlik konsolu aracılığıyla tek bir Kaspersky Lab ürününde sunulur.

Uçtan Uca Güvenlik Özellikleri

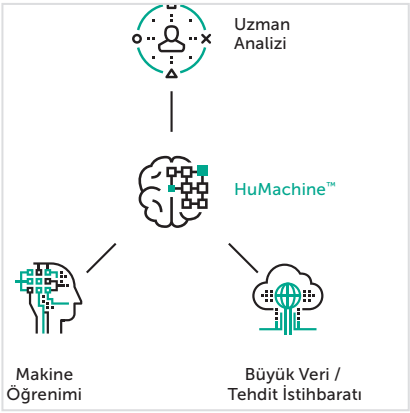
Bu özellikleri dağıtmanın yanı sıra herkese açık ve özel bulut altyapınızda çok katmanlı güvenlik kalitesini ve kapsamını uygulayarak tüm verilerinizin, süreçlerinizin ve uygulamalarınızın kapsamlı "uçtan uca" güvenlik ile korunduğunu bilmenin rahatlığı yaşayabilirsiniz.



Kurumsal BT'nin Geleceğini Koruma

Amazon Web Services, kurumsal BT'yi değiştiriyor. Kaspersky Lab olarak şu anda ve gelecekte hem AWS bulut varlığınızdaki hem de özel bulut ortamınızdaki tüm iş yüklerinizin güvenliğini, görünürlüğünü ve yönetilebilirliğini sağlamaya yardımcı oluruz.

Kaspersky Hybrid Cloud Security, BT ortamınızın dönüşümünü desteklemek ve kolaylaştırmak için sektörde saygın birçok güvenlik teknolojisi sunar, fiziksel ortamdan sanal ortama ve buluta geçişinizin güvenliğini sağlar. Ayrıca görünürlük ve şeffaflık özellikleri, kusursuz bir güvenlik düzenleme deneyimi sunar.



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

#truecybersecurity
#HuMachine

www.kaspersky.com