KASPERSKY lab

Özel Veri Merkeziniz İçin Güvenlik: Doğru Uygulama

www.kaspersky.com.tr
#truecybersecurity

Özel Veri Merkeziniz için Güvenlik: Doğru Uygulama

Bu Belgenin Amacı

Kurumsal veri merkezleri oluşturma yaklaşımı, önemli ölçüde değişmiş ve gittikçe daha fazla yazılım tanımlı hale gelmiştir. Bilgi işlem kaynaklarının sanallaştırılmasıyla ilgili konseptler, uzun yıllardır başarılı bir şekilde kullanılmaktadır. Bu teknoloji, son yıllarda kendine başka endüstrilerde de uygulama alanları bulmuştur. Bu alanlara örnek olarak ağ altyapısı verilebilir. Sanallaştırma teknolojileri, uzun süre önce kurumsal bir standart haline gelmiştir (2016 istatistiklerine göre, sanallaştırma teknolojisinin uygulanması, kurumsal segmentte %75'e ulaşır). Bu geçişin amacı, kurumsal veri merkezi yönetiminin altyapı yerine iş süreçleri tarafından yönetildiği bir düzeye ulaşmaktır.

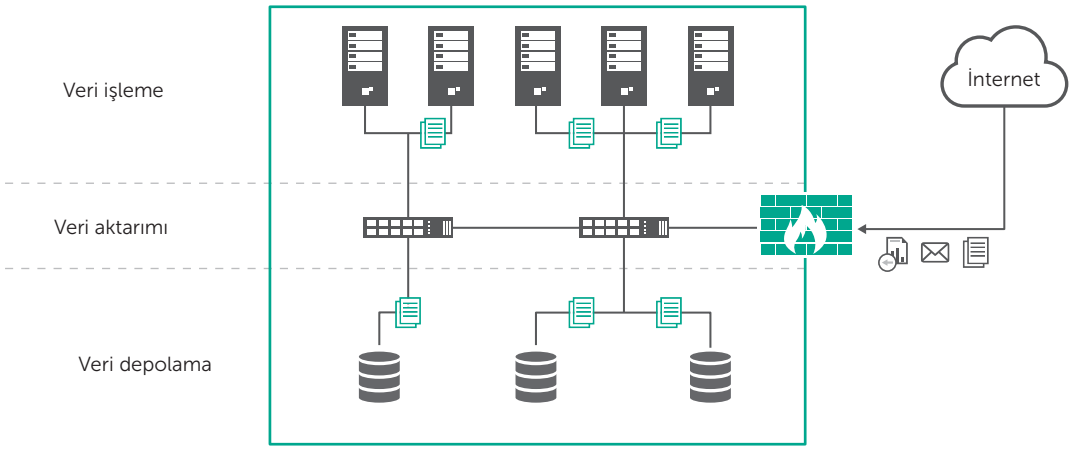
Doğal olarak, tüm bu değişiklikler kurumsal veri merkezleri koruma politikalarının gözden geçirilmesini gerektirir. Veri merkezi teknolojileri yükseltilirken bu tür ilkeleri güncellemek önemlidir. BT güvenliğinin altyapı değişikliklerine ayak uyduramaması veya bu değişikliklere hızlı bir şekilde uyum sağlayamaması, veri merkezinizin korumasını özel çözümlerle değiştirmek için iyi bir nedendir.

Bunu yaparken veri merkezlerinin iş hedeflerine ulaşmak için etkili ve yüksek performanslı bir platform fikri temel alınarak geliştirildiği unutulmamalıdır. Bu nedenle güvenlik çözümleri, asla şirket veri merkezinde kullanılan sistemlerin performansını etkilememelidir.

Kaspersky Lab, kurumsal veri merkezi sistemlerini en gelişmiş siber tehditlere karşı korumak için tasarlanmış özel bir Veri Merkezi Güvenliği çözümü sunar ve veri merkezi sistemleri üzerindeki etkileri en aza indirir.

Kurumsal Veri Merkezi Nedir ve Veri Merkezini Korumak Neden Çok Önemlidir?

Modern dünyada bilgileri işlemek, depolamak ve aktarmak zorunda olmayan bir kuruluş hayal etmek çok zordur. Günümüzde bu işlemlerin tümü kurumsal veri merkezleri tarafından yapılır. Kurumsal bir veri merkezi özel veya herkese açık olabilir. Şirket içinde veya dışında bulunabilir. Ancak veri merkezleri, genellikle herkese açık, özel ve coğrafi olarak dağıtılmış altyapıyı birleştiren çok daha karmaşık bir varlıktır. Her halükârda modern bir veri merkezi, kuruluşun altyapı değişikliklerini daha hızlı takip etmesine ve yeni ortaya çıkan operasyonel görevler



Şekil 1. Veri merkezinin üst düzey mimarisi

için daha etkili bir şekilde kaynak sağlamasına yardımcı olarak şirket faaliyetlerini bir üst düzeye çıkarır.

"Şirketlerin %75'inden fazlası yazılım tanımlı veri merkezleriyle çalışır ve sanallaştırmanın uygulama oranı her geçen yıl artmaya devam etmektedir"

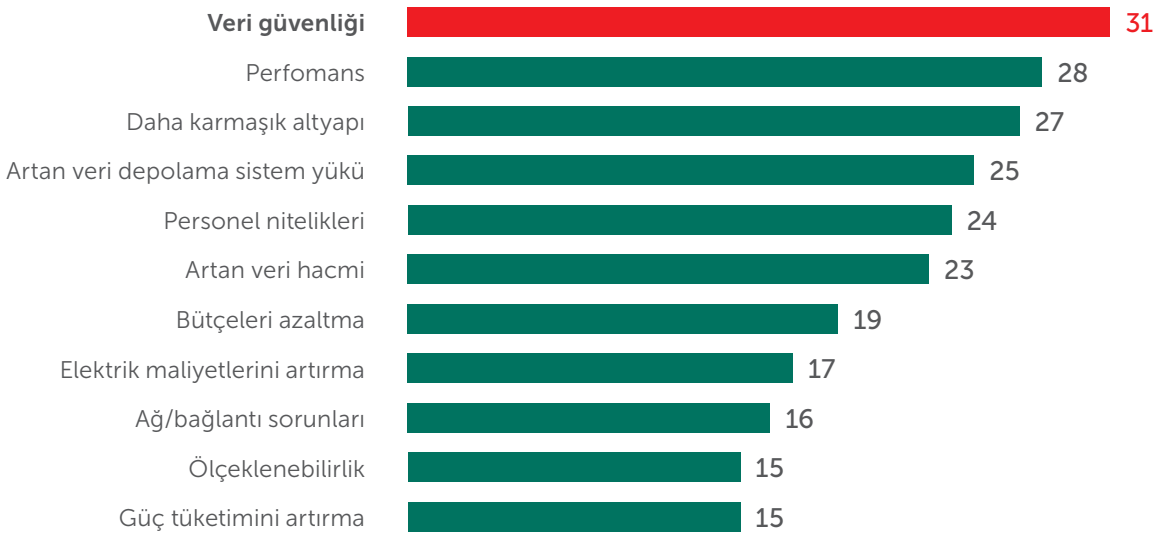
Ancak kurumsal veri merkezleri oluşturmak için modern teknolojiler kullanılsa da veri merkezi altyapılarının düzenlenmesinin temelini oluşturan düşünce yapısı büyük ölçüde gelenekseldir:

- **Veri işleme**: İş uygulamaları için bilgi işlem kaynakları sağlar.
- **Veri depolama**: Şirketin verilerini saklamaktan sorumludur.
- **Veri aktarımı**: tüm iletişim ve veri akışlarını hiçbir sorun olmadan düzenlemenize yardımcı olur.

Tüm bu bileşenler herkese açık, özel veya hibrit olmasına bakılmaksızın tüm veri merkezlerinin verimli çalışması için gereklidir.

Günümüzde kuruluşlar, veri merkezlerini daima yüksek performans ve verimlilik düzeyine sahip olan ve esnek bir şekilde ölçeklendirilebilen güvenilir altyapı ve sistemler olarak görür. Ayrıca kuruluşların veri merkezleri için ek gereksinimleri vardır. Daha fazla kaynağa, daha fazla kontrole, daha fazla güvenilirliğe, daha fazla operasyonel etkinliğe ve daha fazla güvenliğe ihtiyaç duyarlar.

Yakın zaman önce yapılan araştırmalara ve anketlere **göre veri merkezi sahipleri ve büyük şirketler için altyapı güvenliği, veri merkezi faaliyetlerinin en** önemli üç özelliği arasındadır.



Şekil 2. Ana veri merkezi yönetim sorunları[1]

Aynı zamanda şirketler, iş açısından kritik sistemlerini kurumsal veri merkezlerine taşırken, mevcut BT güvenlik konseptlerinin modern bir veri merkezini koruyamayacağı ve bu nedenle mevcut konseptlerini yenilemek zorunda oldukları gerçeğiyle de karşılaşır.

Aslında en önemli sorun, modern veri merkezleri için temel alınan teknolojilerin, yeni kullanıcı etkileşim senaryoları uygulaması ve altyapı bileşenleri arasında ek ara bağlantılar oluşturmasıdır.

"Modern veri merkezlerinin güvenlik yaklaşımı, işletmelerin kendi veri merkezlerini inşa etmeleri için kullandığı teknolojileri dikkate alarak revize edilmelidir."

Güvenlik, modern veri merkezlerinin BT güvenlik konseptini düzeltme motivasyonunun arkasındaki temel etken olmasına rağmen sistem performansını korumak ve altyapının tamamında kolay kontrol sağlamak üst düzey şirket yöneticileri için önemli konulardır.

---

[1] http://www.seagate.com/ru/ru/tech-insights/data-center-management-master-ti/

Veri Merkezinizde Korunması Gereken En Önemli Noktalar

Altyapı açısından bakıldığında modern bir veri merkezi ortamı, birden çok sistemin bir araya getirilmesinden oluşan nispeten basit bir ortamdır.

- Sanal sunucu ve iş istasyonlarını destekleyen ve VMware vSphere, Microsoft Hyper-V, Citrix XenServer veya KVM gibi sanallaştırma platformları kullanılarak oluşturulan veri işleme altyapısı.
- Genellikle doğrudan şirket ağına bağlı dosya sunucularının ve veri depolama sistemlerinin birleşimi olarak düzenlenen kurumsal veri depolama altyapısı.
- Veri merkezi altyapı bileşenleri arasında veri akışı ve etkileşimi sağlayan ve VMware NSX teknolojisi kullanılarak oluşturulanlar dahil olmak üzere sanal ağlar gibi bileşenleri içeren ağ altyapısı.

Tüm bu bileşenler, veri merkezinin etkili bir şekilde çalışmasını sağlamak için kullanılır. Tabii ki bu bileşenlerden her birinin güvenliği, risk altına girebilir.

"Bir veri merkezinin güvenliğini sağlamak için kullanılan araçlar, korudukları teknolojilerin "farkında" olmalıdır."

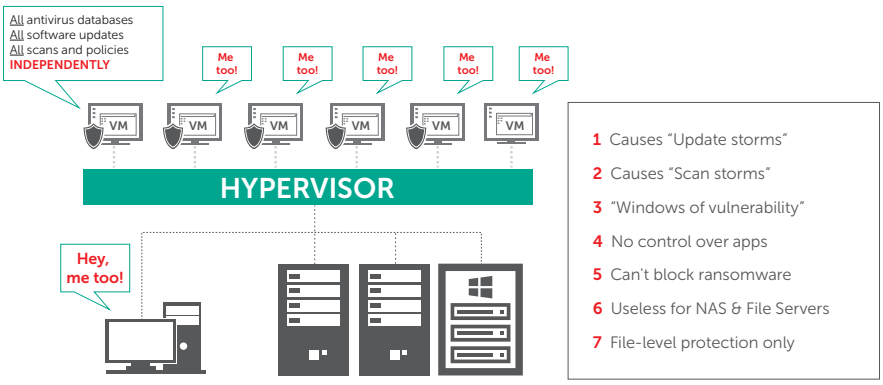
Kaspersky Lab, yukarıdaki bileşenlerin her biri için, veri merkezleri tarafından kullanılan belirli teknolojilere göre geliştirilmiş bir koruma çözümü sağlamayı amaçlar.

Modern Veri Merkezlerinde Ağır Yüklere Neden Olan Koruma Teknolojilerine Yer Yoktur

Bazen fiziksel sunucuları ve iş istasyonlarını korumak için yaygın olarak kullanılan geleneksel çözümler de sanal makinelere dağıtılır. Ancak geleneksel bir güvenlik çözümü, sanal makineye yüklendiğinde kaynakları tüketmeye başlar. Bu nedenle kritik iş uygulamaları, bilgi işlem gücünden daha az faydalandığı için yavaşlar. Bu durumun kullanıcılar tarafından fark edilmesi kaçınılmazdır. Çünkü kullancılar, artık iş görevlerini hızlı ve rahat bir şekilde gerçekleştiremez.

"Veri merkezlerinde sanallaştırma teknolojisinin kullanımıyla kaynaklardan verimli bir şekilde yararlanılması amaçlanır. BT güvenlik çözümleri, bu amaca zarar vermemelidir."

- Sonuç olarak, **her sanal makine** kendi içinde yararlı ancak sanal sunucu düzeyinde gereksiz görevleri yerine getirir. Virüsten koruma veritabanlarını yerel olarak depolar, günceller, kötü amaçlı yazılımlara karşı taramalar gerçekleştirir ve kendini ağ saldırılarına karşı korur.
- Bu görevlerin, her sanal makine için sağlam bir güvenlik sağlayabileceği düşünülebilir. Ancak bu koruma yaklaşımı, her VM'de aşırı yüke neden olur. Sonuçta sanallaştırma **ana bilgisayarında önemli miktarda ek yük oluşur**. Tüm altyapı ve kullanıcılar için verimlilik azalır.
- Virüsten koruma veritabanları aynı anda sanal makineler tarafından indirildiğinde veya planlanan taramalar aynı anda gerçekleştirildiğinde veri merkezinin altyapısında yüksek miktarda yük oluşur. Bu durum, **"güncelleme fırtınalarına"** ve **"tarama fırtınalarına"** yol açar.
- İçinde geleneksel virüsten koruma çözümlerinin yüklü olduğu bir sanal makinenin kapatılması, virüsten koruma veritabanlarının eskimesine yol açar ve yeni kötü amaçlı yazılım saldırıları için **"güvenlik açığı penceresi"** oluşur. Bu sorun, kurumsal veri merkezinin tamamı için ciddi bir tehlike oluşturur.
- Ayrıca geleneksel bir yaklaşım, ağ depolama sistemlerinin ve dosya sunucularının korunması için de kullanışsızdır. Çünkü geleneksel yaklaşım, **tüm dosya işlemlerinin güvenliğini** garanti edemez. Koruma, veri depolama sistemlerinden kullanıcı iş istasyonlarına indirilen dosyaları taramakla sınırlıdır ve ağ klasörlerini **şifreleyici kötü amaçlı yazılımlara (ör. fidye yazılımlar) karşı korumaz.**



Şekil 3. Geleneksel güvenlik çözümlerinin eksiklikleri

Modern Veri Merkezlerinde Tehdit Ortamı

Sanal altyapıları korumak için dağıtılan geleneksel çözümler, kötü amaçlı yazılımlar olmasa bile bu altyapılara zarar verebilir. Bu çözümler, altyapıları yavaşlatır, şirket çalışanlarının işteki görevlerini yerine getirmelerini zorlaştırır ve BT sistemlerinin normal bir şekilde çalışmasını engeller.

Kaspersky Lab tarafından yapılan çalışmalar dahil olmak üzere lider BT güvenlik şirketlerinin araştırmaları, BT güvenlik önlemleri kötü uygulanmışsa veya hiç uygulanmamışsa mevcut tehditlerin birçoğunun en gelişmiş veri merkezleri için bile tehlikeli olduğunu doğrular.

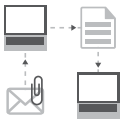
Bu tehlike, modern veri merkezlerinde kullanılan teknolojilerin tehditlere karşı yeterli olmadığını göstermez. Aksine veri merkezlerinde uygulanan yeni çözümler, güvenlik duvarlarında sıfır güven politikaları ve mikro segmentasyon metodolojisi gibi yöntemleri kullanarak altyapının güvenliğini sağlamak için mükemmel fikirleri temel alır. Tüm bunlara rağmen siber saldırılara ve kötü amaçlı yazılımlara karşı veri merkezi koruması, sanallaştırılmış ortamlar ve veri depolama sistemleri için özel olarak geliştirilen özel çözümlere dayalı olmalıdır ve bu çözümler, veri merkezinin tamamı için çok katmanlı koruma sağlayabilmelidir.

Altyapının Tamamı Yeni Koruma Yöntemleri Gerektirir

Modern yazılım tanımlı veri merkezlerinin altyapıları, her geçen gün daha fazla gelişir ve çeşitli iş görevlerini gerçekleştirmek için tasarlanmış çok sayıda sistemi bir araya getirir. Görevler ne kadar çeşitliyse farklı düzeylerdeki sistemler ile kullanıcıları arasındaki bağlantı sayısı da o kadar artar. Tüm altyapı için güvenilir koruma, performansı ve altyapıda devam eden iş süreçlerini etkilemeden sağlanmalıdır. En gelişmiş teknolojiler, veri merkezinin altyapısının karmaşıklığından ve ölçeğinden bağımsız olarak doğru yerde ve doğru zamanda çalışmalıdır.

Sanal Makine Sayısında Kontrolsüz Artış

Çok büyük altyapılarda, sanal makine sayısındaki değişiklikleri kontrol etmek zordur. Sanallaştırma, şablonlar ve kopyalama kullanılarak sanal makinelerin oluşturulmasına olanak sağladığı için güvenlik kesinlikle ihmal edilemez. Basitçe anlatma gerekirse korumasız veya virüslü sanal makinelerin çoğaltılması, toplu arızalara ve kuruluş için ciddi kayıplara neden olabilir. Güvenlik çözümü, veri merkezinizdeki her etkinliğin farkında olmalıdır. Dolayısıyla çözümünüz, güvenliği BT ortamıyla ne kadar çok entegre ederse genel kurumsal güvenlik de o kadar iyi olur.



Ağ Tabanlı Siber Saldırılar

Sanallaştırılmış altyapılardaki ağ etkileşimlerinin çoğu, sanallaştırılmış ağlar aracılığıyla gerçekleşir. Böylece ağ trafiği ve veri akışları, kurumsal ağ altyapısını veya çevresini korumak için tasarlanmış donanıma nadiren ulaşır. Bunun sonucunda pahalı yönlendiriciler ve güvenlik cihazları sanallaştırılmış veri merkeziniz üzerinde tam kontrol sağlayamaz. Sanal ağ İzinsiz Giriş Tespit ve Önleme Sistemi, modern yazılım tanımlı veri merkezleri için bir zorunluluktur.

Beklemeye Alınan Sanal Makineler

Bir sanal makineyi beklemeye aldığınızda veya duraklattığınızda makinenizde yüklü tüm geleneksel uç nokta güvenlik çözümleri, güncelleme yapmayı durdurur. Bu sanal makine, çalışmaya başladıktan sonra modern veri merkezinizin BT güvenlik zincirindeki zayıf halka haline gelir. Ayrıca kapatılmış sanal makinelere de dikkat etmeniz gerekir. Bu makinelerin içinde, VM tekrar açılana kadar bekleyen kötü amaçlı bir yazılım olabilir. Geçerli çalışma durumundan bağımsız olarak tüm VM'leri tarayabilen güvenilir bir çözüme ihtiyacınız vardır.

VDI Sanal Makine Şablonuna (Golden Image) Yönelik Tehditler

Masaüstü sanallaştırma teknolojisi, birçok avantaj sunar ve verimliliği artırır. Birkaç dakika içinde yüzlerce sanallaştırılmış masaüstü bilgisayar oluşturmak için tek bir sanal makine şablonu (golden image) kullanılabilir. Ancak, sanal makine şablonunun (golden image) zarar görmesi veya şablona virüs bulaşması, kullanıcıların iş açısından kritik verilerle çalışmak için kullanacağı yüzlerce tehlikeli sanal makinenin oluşturulmasına neden olabilir. Ayrıca güvenlik sistemleriniz güncellendiği için VDI yöneticilerinizden her gün "sanal makine şablonlarını" güncellemelerini isterseniz yöneticileriniz bu durumdan hiç memnun olmayacaktır. Bu işlem onlar için

kaynak açısından yoğun bir görevdir. Güvenlik çözümünüzün, kaynakların bu şekilde boşa kullanılmasını önleyen doğru bir mimariye sahip olması ve aynı zamanda her VDI makineniz için optimum düzeyde koruma sağlamaya devam etmesi gerekir.

Tehdit Altındaki Veri Depolama Sistemleri

Birçok modern ağa bağlı depolama (NAS) cihazı ve popüler dosya sunucuları, genişletilmiş veri koruma özellikleri sunar. Ancak kritik veriler için özel olarak tasarlanmış ek bir çözüme ihtiyaç vardır. Bu çözüm, özellikle veri depolama sistemleri için geliştirilmiş olmalı ve sistem performansını düşürmemelidir. Ayrıca geleneksel çözümlerin altyapınızdaki tüm dosyaları tarayacağını da garanti edemezsiniz. Bazı tehditler, iş kullanıcılarınızın bilgisayarlarındaki uç nokta güvenlik çözümlerinden gizlenebilir. Doğrudan depolama cihazıyla entegre olabilen ve kaynağına bakılmaksızın her dosya işlemini yani depoya giren ve çıkan her şeyi "görebilen" bir güvenlik çözümüne ihtiyacınız vardır.

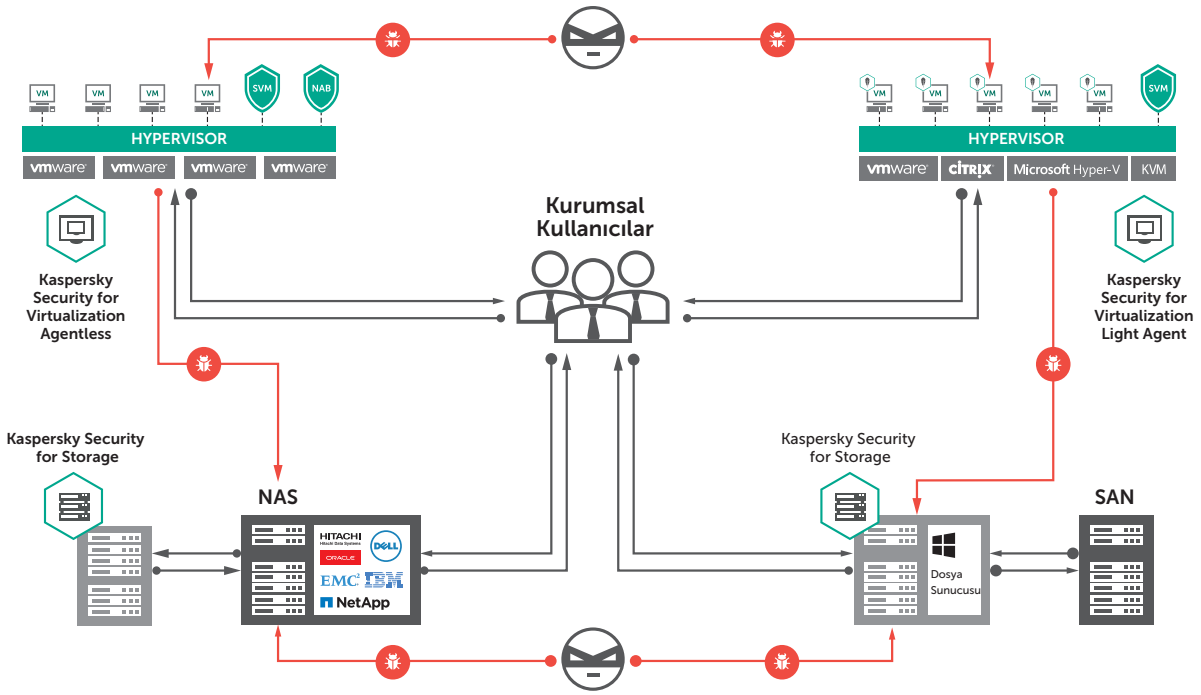
Aşırı Kaynak Tüketimi

Modern yazılım-tanımlı veri merkezlerinin altındaki düşünce, sistemlerin verimliliğini artırma ve bilgi işlem kaynaklarının yüksek konsantrasyonunu sağlama ilkesi üzerine kuruludur. "Ağır" bir güvenlik çözümünün yüklenmesi, her sanal makinede büyük bir yük oluşturarak sanallaştırma ana bilgisayarlarındaki (hipervizörler) kaynak kullanımını önemli ölçüde artırır. Kötü seçilmiş bir güvenlik çözümü, işletmenin kendi modern yazılım tanımlı veri merkezini kurma projesini başlatırken hedeflediği avantajların tamamını kolaylıkla yok edebilir.

Modern Veri Merkezinizi Koruma

Kaspersky Lab, modern veri merkezlerine yönelik olarak hem sanallaştırılmış ortamlar (sanallaştırılmış sunucular ve uç noktalar) hem de kurumsal veri depolama sistemleri için koruma sağlayan özel bir güvenlik çözümü sunar. Çözümün bileşenleri olan Kaspersky Security for Virtualization ve Kaspersky Security for Storage çözümleri, başlangıçtan itibaren kurumsal veri merkezleri oluşturmak için kullanılan teknolojilerle entegre olmak ve kaynakların optimum düzeyde kullanılmasını sağlamak için tasarlanmış ve geliştirilmiştir.

Çözümün benzersiz mimarisi, modern veri merkezlerinin çalışma şekli göz önünde bulundurularak geliştirilmiştir. Çözümün sistem performansı üzerinde minimum etkiye sahip olmasına dikkat edilmiştir. Böylece yüksek konsolidasyon oranlarının sürdürülmesi ve kurumsal veri merkezi oluşturma projesinde iş verimliliğin



Şekil 4. Çözümün Mimarisi

artırılması hedeflenmiştir. Çözümün önemli bir avantajı, veri merkezinde kullanılan teknolojiler ile entegrasyonu ve tek bir konsoldan merkezi yönetim sağlamasıdır. Bu avantajlar, sistem yöneticilerinin güvenlik ilkelerini daha hızlı bir şekilde uygulamasına yardımcı olur.

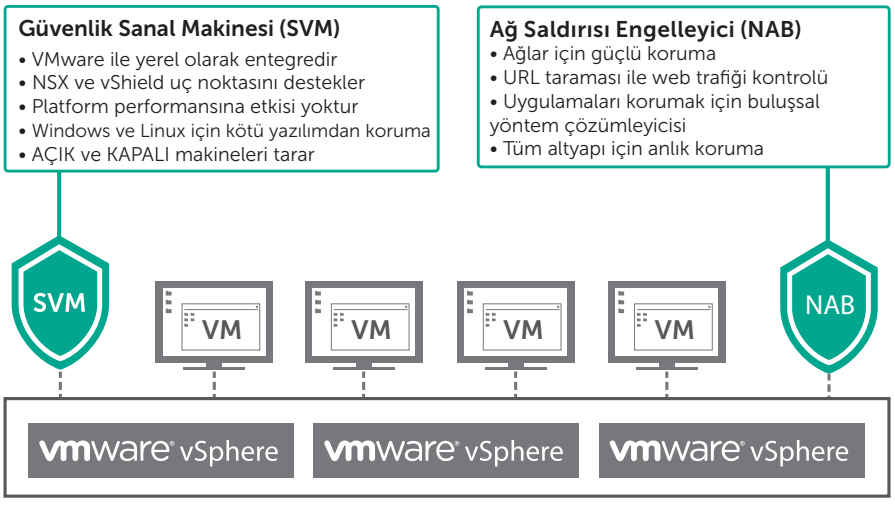
Kaspersky Security for Virtualization: VMware NSX for vSphere Platformunu Hazırlama

NSX teknolojilerine sahip VMware vSphere platformu, yazılım tanımlı bir model kullanarak veri merkezinin ağını yeniden oluşturur. Bu sayede birkaç saniye içinde ağ topolojisini oluşturmayı veya yeniden yapılandırmayı ve "sıfır güven" modeline dayalı bir veri merkezi güvenlik stratejisini hızlı bir şekilde uygulamayı sağlar. Kaspersky Lab ve VMware'in ortak çözümü, modern veri merkezi altyapısı için entegre koruma sağlama görevini kolaylaştırır.

Entegre VMware NSX hizmetleri	
Dağıtımlı Güvenlik Duvarı	Sanal ağlar (VXLAN)
Sunucu Etkinliği İzleme	VPN (IPSec, SSL L2VPN)
Kaspersky Security For Virtualization	
Kötü Amaçlı Yazılımdan Koruma	Sanal Ağ IDS/IPS
Güvenlik Otomasyonu	Politika Tabanlı Entegrasyon
Güvenlik Etiketleri Entegrasyonu	Kapatılmış VM'ler İçin Bile Eksiksiz Altyapı Taraması

Kaspersky Security for Virtualization Agentless, Vmware teknolojilerine dayalı yazılım tanımlı veri merkezlerini korumak için özel olarak tasarlanmıştır. Korunan VM'lere ek aracının yüklenmesi gerekmez ve sanallaştırılmış ortam için "gereksiz" olan süreçler, dosya ve ağ trafiği tarama işlevlerini sağlayan özel güvenlik cihazlarına aktarılır. Bu avantajlar sayesinde çözümün yazılım tanımlı veri merkezi sistemleri üzerindeki etkisi minimum düzeydedir ve her VM, başlatılır başlatılmaz koruma altına alınır.

"Kaspersky Security for Virtualization Agentless, geleneksel çözümlere kıyasla %40 daha az VM belleği tüketir ve %80 daha az disk alanı kaplar. Sonuç olarak iş sistemleri verimli ve güvenli bir şekilde işletilir."



Şekil 5: Aracısız güvenlik çözümü

Çözüm, özel bir API aracılığıyla VMware altyapısıyla etkileşim kurar. Böylece her sanal makine için kötü amaçlı yazılımlara karşı koruma sağlamanın yanı sıra ağ tehditlerini tespit eder ve engeller. Ayrıca altyapı içinde gerçekleşen süreçlerle derin entegrasyon sağlar.

- **Otomatik dağıtım**, BT ve BT güvenlik personelinin çalışmasını oldukça kolaylaştırır. Her VM için tanımlanan güvenlik ilkelerine göre hipervizörlerde güvenlik cihazlarının tam otomasyonunu sağlar.
- **Sıkı güvenlik ilkesi entegrasyonu**, her VM'nin kurumsal BT güvenlik ilkesi tarafından belirlenen koruma işlevselliğine sahip olması anlamına gelir.
- **NSX Güvenlik Etiketleri ile entegrasyon**, altyapı ile koruma sağlayan araçlar arasındaki "iletişimin" sınırlarını genişletir. Böylece veri merkezinin, BT güvenlik olaylarına zamanında ve otomatik bir şekilde yanıt vermesini sağlayarak saniyeler içinde yönetim kararları verir ve yazılım tanımlı veri merkezinin ağ topolojisini yeniden yapılandırır.
- **Hem çalışan VM'ler hem de kapalı olanlar**, tamamen aracısız modda tarandığı için kurumsal veri merkezinin tamamı 7/24 korunur.

Çözümün mimarisi, başlangıçtan itibaren iş açısından kritik sunucuların çalışmasına hiç etki etmemesi ve gelişmiş koruma sağlaması için tasarlanmıştır.

Patentli Hafif Aracı Teknolojisi

Kurumsal veri merkezlerinde barındırılan bazı sanallaştırılmış ortamlar, altyapıyı güvenlik çözümüne bağlayan entegrasyon protokollerine sahip değildir. Ancak bu tür ortamlarda güvenliği sağlamak çok önemlidir.

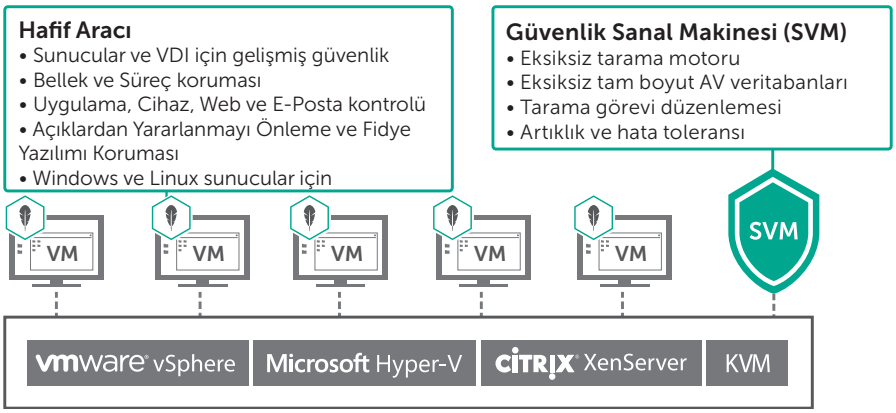
Ayrıca sanal masaüstü altyapıları (VDI), kullanıcının ilgili tehditlerin ve önleme yöntemlerinin ne kadar farkında olduğuna bakılmaksızın her kullanıcıya güvenilir koruma sağlayan teknolojiler gerektirir.

"Hafif Aracı, program yürütmeyi kontrol eder ve sanal uç noktaları şifreleyici virüsler ve diğer tehditlere karşı korur."

Kaspersky Security for Virtualization Light Agent, aracı çözümün ilkelerine sahip olmasına rağmen ek koruma katmanları sağlar. Çözüm, VMware vSphere, Microsoft Hyper-V, Citrix XenServer ve KVM dahil olmak üzere en popüler sanallaştırma platformlarını destekler. Tüm sanal uç noktalara, VMware Horizon ve Citrix XenDesktop gibi VDI platformlarının performansını muhafaza eden yepyeni koruma araçlarının ve teknolojilerinin birleşimini sunar.

- Sanal sunucular ve VDI için kötü amaçlı yazılımlara karşı koruma ve IDS/IPS
- VMware, Citrix, Microsoft ve KVM platformları için güvenlik
- XenDesktop ve Horizon için güçlü ve hafif güvenlik
- Altyapınız ile birlikte çalışarak, özelliklerini güçlendirir.
- Performansı hiç etkilemeyen mükemmel şekilde dengelenmiş koruma

Güvenlik Sanal Makinesi (SVM) adı verilen özel koruma sunucusu, tüm VM'lerin merkezi olarak taranmasını sağlar. Aynı zamanda, her VM'de yüklü olan Hafif Aracı, dosyalara ek olarak makinenin bellek ve süreçlerinin taranmasını sağlar. Hafif Aracı'yı VDI makinelerine dağıtmak e-posta ve internet trafiğini analiz eden



Şekil 6. Hafif Aracı'nın çalışma prensipleri

sezgisel modüllerin yanı sıra Uygulama Kontrolü, Cihaz Kontrolü ve URL Kontrolü gibi gelişmiş güvenlik özellikleri etkinleştirir. Ayrıca, Hafif Aracı'nın temel aldığı patentli koruma teknolojileri, uç noktaların şifreleyici virüsler dahil olmak üzere gelişmiş saldırılara karşı korunmasını sağlar.

Veri Merkezlerindeki Kurumsal Veri Depolama Sistemlerini Koruma

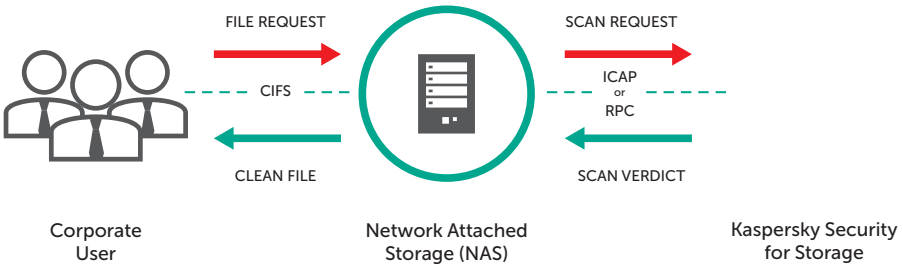
Sanallaştırılmış sunucular ve iş istasyonları gibi uç noktalarda kullanılan en gelişmiş koruma teknolojilerinde bile büyük bir kısmı kurumsal veri merkezlerinde depolanan verileri korumak gibi sorunlar özel koruma araçlarıyla çözülmelidir.

Kaspersky Lab, ICAP ve RPC protokolleri aracılığıyla çok sayıda kurumsal ağa bağlı veri depolama sistemleriyle entegre edilen ve her dosya işlemi için sağlam, yüksek performanslı ve ölçeklenebilir koruma sağlayan **Kaspersky Security for Storage** çözümünü sunar. Yüksek performanslı bir motorla birleştirilmiş olan çözümün mimarisi, önemli kurumsal dosyalara kötü amaçlı yazılım bulaşması ile ilgili olası riskleri sıfıra indirir.

"Depolama sistemleri için güvenlik çözümü, yalnızca ağa bağlı depolama sistemlerini değil aynı zamanda dosya sunucularını da korur."

Hangi kullanıcının hangi dosya etkinliğini gerçekleştirdiğinin hiçbir önemi yoktur. Tüm işlemler, Kaspersky Security for Storage çözümünün virüsten koruma altyapısı tarafından işlenir.
Kaspersky Lab tarafından geliştirilen güçlü virüsten koruma motoru, başlatılan veya değiştirilen dosyaları virüsler, solucanlar ve Truva Atları dahil olmak üzere her türlü kötü amaçlı yazılım türü için tarar. Gelişmiş sezgisel analiz yeni ve bilinmeyen tehditleri bile tanımlayabilir.

Çözüm, tarama işleminin dışında tutulacak "güvenilir bölgeler" özelliğinin yanı sıra belirli dosya biçimlerini ve yedek kopyalama gibi süreçleri destekler.



Özet

Kaspersky Lab, yazılım tanımlı veri merkezinizin her parçasını korumak için kötü amaçlı yazılımlara karşı ödüllü koruma sağlayarak en yüksek düzeyde sistem verimliliği sunar. Çözüm VMware vSphere with NSX, Microsoft Hyper-V, Citrix XenServer ve KVM dahil olmak üzere tüm lider hipervizörler için koruma sağlar ve VMware Horizon ve Citrix XenDesktop gibi masaüstü sanallaştırma endüstrisi standartlarına entegredir.

Sanallaştırma platformları için özel güvenlik sağlamanın yanı sıra, Ağa Bağlı Depolama (NAS) ve kurumsal dosya sunucularını korumak için bir çözüm sunarız. Böylece kaynağına bakılmaksızın her türlü dosya etkinliğini koruma altına alırız.

Kaspersky Data Center Security çözümü, güvenli ve etkili bir sanal ortam oluşturmak için güçlerin birleştirilmesini sağlayarak veri merkezi altyapınızın ve güvenliğinin birlikte çalışma şeklini yeniden tanımlar. Kaspersky Data Center Security çözümü, entegrasyon özellikleri sayesinde sanal ortamınızı gelişmiş koruma özellikleriyle tanıştırır. Ayrıca verilerinizin tam olarak nasıl ve nerede depolandığını gösterir ve her bir dosya işleminizin güvenliğini sağlar. Böylece kurumsal veri merkeziniz, 7/24 tamamen erişilebilir ve güvenli durumda kalır.

Kaspersky Lab
Kurumsal Güvenlik: **www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliğiyle İlgili Haberler: **business.kaspersky.com.tr/**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr