Kaspersky®
Secure Hypervisor

Kaspersky Secure Hypervisor: Tehditlere sıfır tolerans

Çözümün amacı, tek bir fiziksel makinede birden çok sanal makine (konuk işletim sistemi) çalıştırmayı mümkün kılmak ve fiziksel kaynakları konuk sistemler arasında dağıtmaktır.

Giriş

Profesyonel hacker'ların ve APT'lerin günlük hayatın bir parçası haline geldiği bir dünyada gömülü sistemlerin benimsenmesi ve başarısı konusunda güvenlik en önemli etkenlerden biridir. Tehditler; açık arayüzlere yapılan saldırılardan, çevre birimlerine (ör. PCI, USB) karşı belgelenmemiş veya saldırgan davranışlara kadar değişiklik gösterebilir. Başarılı bir saldırıdan sonra saldırgan, işletim sistemi güvenlik açıklarını kullanarak ilerleyebilir ve kritik süreçleri tehdit edebilir. Genel amaçlı sistemlerin güvenlik açıklarına ve geniş saldırı yüzeyine rağmen, satıcılar yazılımın kolay erişilebilirliği nedeniyle popüler platformları tercih etmektedir.

Sanallaştırma teknolojisi, mevcut kod tabanını yeniden kullanma özelliğini korurken sistem güvenliğini güçlendirme fırsatı sunar.

Amaç

Kaspersky Secure Hypervisor, KasperskyOS mikroçekirdeği üzerinde çalışan ve güvenlik özelliklerini kullanan tip 2 hipervizördür ve KasperskyOS işletim sistemini bir hipervizör çözümüne dönüştürür.

Çözümün amacı, tek bir fiziksel makinede birden çok sanal makine (konuk işletim sistemi) çalıştırmayı mümkün kılmak ve fiziksel kaynakları konuk sistemler arasında dağıtmaktır. Sanallaştırma, normalde konuk işletim sistemlerinin fiziksel makineye yakın bir performans göstermesini sağlayan modern CPU özellikleri tarafından desteklenir.

Sanallaştırma çözümünün temel avantajı, güvenilir olmama ihtimali olan konuk işletim sistemlerinin birbirinden ve aynı fiziksel makinede bulunan kritik hizmetlerden ayrılmasıdır. Böylece saldırı yüzeyi küçültülür ve yararlanılan güvenlik açıklarının olası etkisi en aza indirilir. Hipervizör, konuk işletim sistemi etkinliklerinin kritik hizmetlere veya hipervizörün kendisine zarar veremeyeceği şekilde konuk işletim sistemi eylemlerinden korunur.

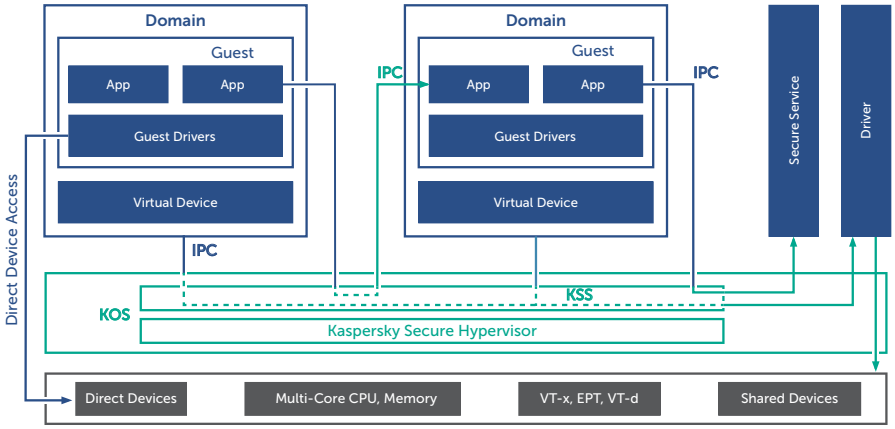
Özellikler

Kaspersky Secure Hypervisor, iki yazılım bileşeni içerir. Bu bileşenlerden biri ayrıcalıklı çekirdek modunda çalışırken diğeri kullanıcı modunda çalışır. Ayrıcalıklı çekirdek bileşeni kaynakların yönetiminden sorumludur (ör. bellek, CPU) ve G/Ç (I/O) cihazlarına erişim sağlar. Kaspersky Secure Hypervisor çözümünün kullanıcı modu bileşenleri, ortak ana bilgisayar kullanıcı modu cihaz sürücüleri ve KL secdev adı verilen ve etki alanları arasında veya bir etki alanı ile hipervizör arasında iletişim kanalları sağlayan özel bir konuk sürücü içerir.

Cihaz emülasyonunun güvenlik avantajlarından biri, hipervizörün konuk işletim sistemi ve cihaz arasındaki tüm işlemleri engelleyebilmesi ve konuk işletim sisteminin devre dışı bırakamayacağı ek güvenlik önlemleri uygulamasıdır

Kaspersky Secure Hypervisor, ortak bir CPU ve bellek paylaşan sanal ortamlar (etki alanları) oluşturmak amacıyla donanım cihazları için sanallaştırma desteği kullanır. Donanım sanallaştırma özellikleri, mevcutsa PCI cihazlarını (video adaptörü, ağ adaptörü, sabit disk denetleyicisi, USB gibi) konuk işletim sistemine doğrudan geçirmek için kullanılabilir. Bu teknik, cihazların performansını artırır ancak paylaşım olasılığını ortadan kaldırır. Aşağıda emülasyon veya doğrudan geçiş tekniği kullanılan cihazların listesini görebilirsiniz.

Cihazların paylaşılması gerekiyorsa kullanıcı alanı cihaz emülasyon tekniğini kullanırız. Bu teknikteki amaç paylaşılması gereken cihaza doğrudan erişimi olan bir KasperskyOS kullanıcı alanı sürücüsünü çalıştırmaktır. Sürücü cihaz emülasyonu yöntemini kullanır. Bu yöntem, konuk işletim sistemi cihazın sanal olduğunu bilmeden cihaza erişim sağlamak için kullanılabilecek bir konuk işletim sistemi arabirimi sağlar. Cihaz emülasyonunun güvenlik avantajlarından biri, hipervizörün konuk işletim sistemi ve cihaz (ör. ağ kartı, SATA denetleyicisi) arasındaki tüm işlemleri engelleyebilmesi ve konuk işletim sisteminin devre dışı bırakamayacağı ek güvenlik önlemleri (ör. trafik filtreleme, şifreleme) uygulamasıdır. Cihaz emülasyonu, aynı zamanda donanım sanallaştırma özelliklerinin kullanılamadığı yerlerde kullanılabilir.



Araç İçi Bilgi ve Eğlence Sistemi

Bu mimaride, iki etki alanı kullanılır. Bunlardan birisi görev açısından kritik yazılımlara (araç kontrolü, ağ yazılımı) ve diğer kritik olmayan bilgi-eğlence yazılımlarına (medya, bağlanabilirlik, ses özellikleri, kullanıcı arabirimi) yöneliktir. Ayrı sanal ortamlar, kullanıcının gerçekleştirdiği eylemlerden bağımsız olarak görev açısından kritik yazılımların dengesini korur. Cihaz emülasyonu tekniğiyle paylaşılan donanım (ağ kartı, GSM veya Wi-Fi modülleri gibi), etki alanları tarafından kullanılabilir ve donanım maliyetleri azaltılabilir. Bu mimari, aynı zamanda yazılım güncellemeleri sırasında kritik bileşenleri etkilemeden bilgi eğlence yazılımının güncel kalmasını sağlar.

Endüstriyel Güvenlik Sistemleri

Bu mimaride, endüstriyel yazılımları, iletişim yazılımını, veritabanlarını ve kullanıcı arabirimlerini ayırmak için iki veya daha fazla etki alanı kullanılır.

Mobil Cihazlar

Hipervizör çözümü, (1) kurumsal veriler ve kritik uygulamalar (örneğin, geniş bant yazılım yığını, VPN, güvenlik hizmetleri, sertifikalar ve kredi kartları için depolama) ve (2) kişisel veriler için etki alanlarını veya profilleri ayırabilir. Bu yaklaşım, gizli iş verilerini, iletişimleri ve özel bilgileri birbirinden ayırmaya yardımcı olur.

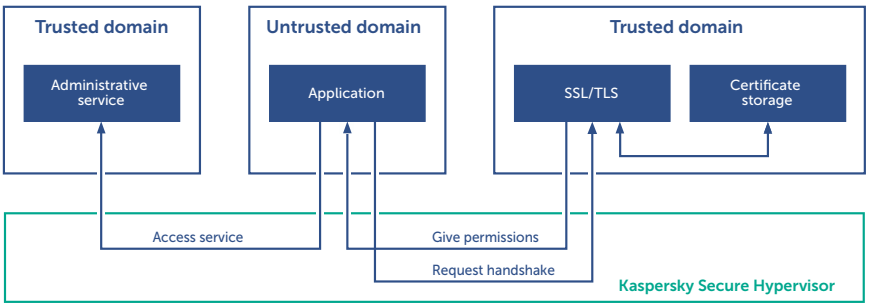
Uygulama

Kaspersky Secure Hypervisor çözümünü aşağıdakiler için güvenilir bir sistem olarak görüyoruz:

- Nesnelerin İnterneti
- Otomobiller
- Sağlık
- Endüstriyel otomasyon
- Satış noktası bilgisayarları
- İnce istemciler ve VDI'lar
- Kurumsal tabletler ve akıllı telefonlar

Sertifikalar ve Anahtarlar İçin Güvenli Depolama

Bu mimaride, sertifika depolama ve şifreleme hizmetleri ayrı ve güvenilir etki alanlarında tutulur. Konuk işletim sistemi uygulamaları, başka bir etki alanında çalışır ve şifreleme hizmetlerine Kaspersky Secure Hypervisor iletişim kanalları aracılığıyla erişim sağlar. Güvenilir bileşenler, uygun kimlik doğrulaması ile konuk işletim sistemi uygulamalarına ek ayrıcalıklı izinler verebilir (ör. yönetim hizmetleri izni). Konuk işletim sistemi, uygulamaları ele geçirilmiş olsa bile hipervizör tarafından sağlanan güvenlik ilkesi uygulama ve etki alanı ayırma özellikleri nedeniyle anahtarlara erişim sağlayamaz veya ayrıcalıklarını artıramaz.

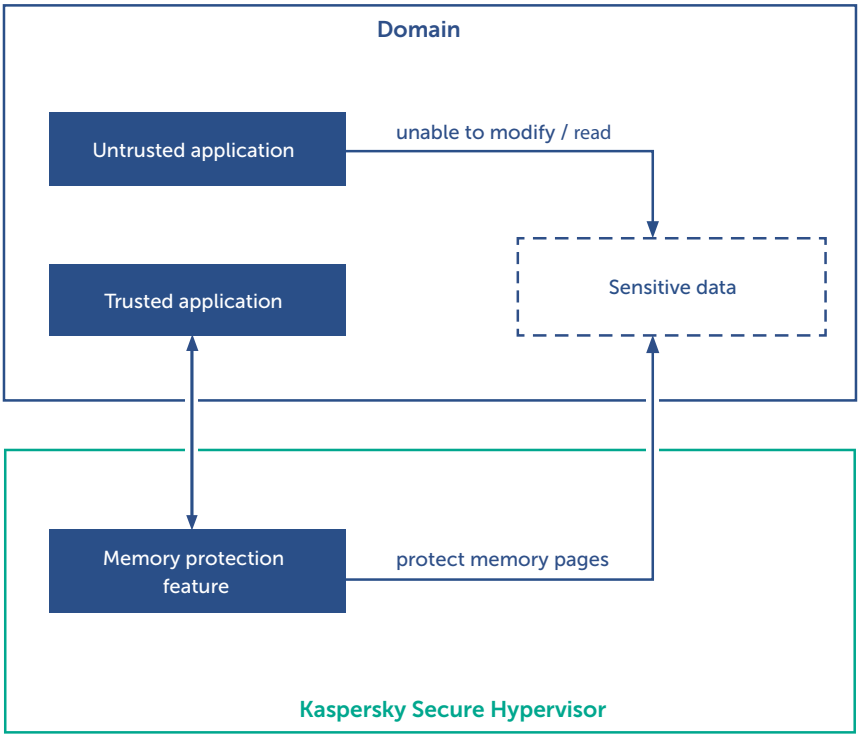


Ağ Analizi ve Filtreleme

Bu mimaride, konuk işletim sistemi uygulamaları ile dış dünya arasındaki tüm ağ iletişimi, şeffaf bir şekilde filtrelenir (Konuk işletim sistemi uygulamalarında değişiklik yapılmaz ve konuk işletim sistemi uygulamaları filtrelemenin farkında olmaz). Gerekirse konuk işletim sistemi uygulamalarından gelen olası saldırılara karşı görünmez kalmak için trafik denetimi uygulanabilir. Konuk işletim sistemi uygulamaları, ele geçirilse bile filtreleme işlemini devre dışı bırakamaz ve verileri uzak bir tarafa gönderemez.

Hassas Konuk İşletim Sistemi Verilerinin Korunması

Kaspersky Secure Hypervisor, bellek koruma mekanizması sayesinde konuk işletim sisteminin hassas verilerini değişimlere veya yetkisiz erişime karşı korur. Bellek koruması, konuk fiziksel sayfalarında uygun izinleri belirleyerek gerçekleştirilir. Tipik bir senaryoda, konuk işletim sistemi, güvenilir olmayan bir



Teknik gereklilikler

- **Ana bilgisayar işletim sistemi.** Kaspersky Secure Hypervisor, ana bilgisayar sistemi olarak KasperskyOS ile birlikte temin edilen tip 2 hipervizördür.
- **Platformlar.** VT-x ve (isteğe bağlı) VT-d teknolojisi desteğiyle Intel x86 veya x64. ARM desteğiyle ilgili çalışmalar devam etmektedir.
- **Konuk işletim sistemleri.** Ubuntu ve CentOS gibi değiştirilmemiş Linux tabanlı dağılımlar, hem x86 hem de x64 versiyonlarında konuk işletim sistemi olarak kullanılabilir. Diğer konuk ortamları desteği (öncelikle Windows) için çalışmalar devam etmektedir.
- **Emülasyon tekniği kullanılan cihazlar.** x86 eski (PIC, PIT), PCI veriyolu, NE2000, IDE/ SATA denetleyicisi, UART (COM bağlantı noktası).
- **Test edilen doğrudan geçiş cihazları.** USB denetleyicisi, SATA denetleyicisi, PCI Ethernet, Radeon/nVIDIA video kartları, eski IDE denetleyicisi.

Patentler

KasperskyOS ve Kaspersky Security System çözümlerinin temelini oluşturan teknolojiler, birden çok patent kapsamındadır:

US 7386885 B1, US 7730535 B1,
US 8370918 B1, EP 2575318 A1,
US 8522008 B2, US 20130333018 A1,
US 8381282 B1, EP 2575317 A1,
US 8370922 B1, EP 2575319 A1,
US 9015797 B1, DE 202014104595 U1

uygulama çalıştırmadan önce konuk işletim sisteminin hassas verilerini korumak için Kaspersky Secure Hypervisor çözümüne çağrı yapar. Korunabilir verilere örnek olarak konuk işletim sistemi çekirdek kodu, konuk güvenlik hizmetleri ve yapılandırmalar verilebilir.

Avantajlar

1. **Özel çözüm.**
   Kaspersky Secure Hypervisor, Kaspersky Lab tarafından tam olarak desteklenen özel bir çözümdür. Geliştirme süreci, sistematik test ve doğrulama ile en iyi uygulamalara dayanmaktadır.
2. **Güçlü izolasyon ve aracılı iletişim.**
   Kaspersky Secure Hypervisor, KasperskyOS özelliklerinden faydalanarak tek bir makinede birden çok konuk işletim sistemini ve KasperskyOS yerel uygulamalarını çalıştırmak için bir yöntem sağlar. Etki alanları arasındaki izolasyon, Kaspersky Secure Hypervisor çözümünün çekirdek bileşeni tarafından gerçekleştirilir. Etki alanları ve bir etki alanı ile çekirdek arasındaki tüm iletişim, Kaspersky Security System aracılığıyla önceden tanımlanmış bir güvenlik ilkesine göre sağlanır. Bir saldırgan, sanal makineden çıkış işlemini gerçekleştirse bile güvenlik ilkesi sonraki eylemleri engeller.
3. **Esnek erişim kontrolü.**
   Kaspersky Security System, öznitelik temelli bir model üzerine kurulmuştur ve çok çeşitli ilkeleri (ör. nesne özellikleri, akış kontrolü, Type Enforcement ve çok düzeyli güvenlik) destekler. Esnek ve genişletilebilir yapısı, bir uygulama alanıyla ilgili özel etki alanı ilkeleri geliştirmeyi mümkün kılar.
4. **Konuk işletim sistemi için kaynak yönetimi.**
   Kaspersky Secure Hypervisor, ortamın tamamını konuk sistemlerden gelen olası kaynak tüketme saldırılarına karşı korumak için konuk sistemlerin kullanabileceği kaynak miktarını (bellek veya fiziksel cihaz erişimi gibi) sınırlandırır. Tehlikeli olabilecek harici cihazlar kısıtlanabilir. Bu sayede hatalı veya kötü amaçlı donanımlar, konuk işletim sistemlerinin veya hipervizörlerin belleğine erişemez.
5. **Güvenli önyükleme sistemiyle entegrasyon özelliği.**
   Kaspersky Secure Hypervisor, hipervizörün ve konuk işletim sisteminin bütünlüğünü koruyan özelliklere sahiptir.
6. **Küçük güvenli bilgi işlem tabanı.**
   Kaspersky Secure Hypervisor, ana bilgisayar işletim sistemi olarak KasperskyOS ile kullanıldığında KasperskyOS'nin mikroçekirdek tasarımından faydalanır ve küçük bir doğrulanabilir güvenli bilgi işlem tabanı (TCB) sağlar*. Tüm cihaz sürücüleri bir ana bilgisayar kullanıcı modunda çalıştırılarak hipervizörün zarar görmesi veya ele geçirilmesi riskini azaltılır.

*Güvenli bilgi işlem tabanı (TCB), çözümün genel güvenliği için önemli olan tüm bileşenlerin (donanım, ürün yazılımı ve yazılım) kümesidir. Küçük TCB, kapsamlı test ve doğrulama işlemlerini kolaylaştırır.

www.kaspersky.com.tr

Daha fazla bilgi için şu adresi ziyaret edin: **os.kaspersky.com**
İnternet güvenliği hakkında her şey için: **www.securelist.com**