kaspersky GELECEĞİ YAKALAYIN

Kaspersky Sandbox

Kurum içerisine BT güvenliği uzmanları almanıza gerek kalmadan bilinmeyen ve gizlenmeye çalışan tehditlere karşı korunmanız için gelişmiş tespit yeteneği

Günümüzde yapılan gelişmiş siber saldırılar, şirketleri paralize edecek ve finansal ve tanınırlık yönünden zarara uğratacak güce sahiptir. Karmaşık tehditlerin finansal varlıkların ve ticari sırların çalınmasına, verilemeyen hizmetler nedeniyle müşteri güveninin kaybedilmesine ve diğer birçok olumsuz etkiye neden olması iş stabilitesi ve başarısını önemli ölçüde etkiler. Çok hızlı biçimde şekilde değiştiren siber saldırıları önlemek için, çevre ağını (güvenlik duvarları, e-posta/web geçitleri, proxy sunucuları), iş istasyonlarını ve sunucuları (antivirüs koruması ve temel işlevselliğe sahip Uç Nokta Koruma sınıfı çözümler) korumak üzere tasarlanan geleneksel araçlar tek başlarına yetersiz kalmaktadır. Bu nedenle, ileri görüşlü şirketler karmaşık vakaları tespit etmek, araştırmak ve yanıtlamak için özelleştirilmiş araçlar edinmeyi göz önünde bulundurmalıdır.

Kaspersky Sandbox çözümünün uygun olduğu kuruluşlar:

- BT güvenliği rolünü BT departmanının üstlendiği, özel bir güvenlik ekibi olmayan şirketler.
- Ek bir BT güvenliği oluşturmak istemeyen küçük ölçekli işletmeler.
- Coğrafi açıdan dağıtılmış bir altyapıya sahip olan ve tesis içi BT güvenlik uzmanları bulunmayan büyük ölçekli şirketler.
- Tam zamanlı BT güvenliği analistlerinin kritik görevlere odaklanmasına gereksinim duyan şirketler.

Kaspersky, 20 yılı aşkın süredir her ölçekte, sektörde ve BT güvenliği gelişmişlik düzeyindeki şirketler için koruma araçları sunmaktadır. Sürekli olarak yaptığımız araştırma ve geliştirme çalışmaları ile tehdit avcılığı, araştırması ve yanıtları alanında attığımız adımlar sayesinde, Kaspersky siber suçla mücadelede en ön saflarda yer almaktadır.

Kaspersky'nin karmaşık tehditlerle mücadele amacıyla sunduğu ürün ve hizmet portföyü şunlardan oluşur:

- Kaspersky Anti Targeted Attack, karmaşık tehditleri ve hedefli saldırıları ağ düzeyinde tespit edip araştırmak için kullanılan son teknoloji çözüm.
- Kasperky Endpoint Detection and Response, iş istasyonları ve sunuculara yönelik karmaşık siber tehditleri tespit etmek, araştırmak ve yanıtlamak için kullanılan bir çözüm
- Kaspersky Tehdit İstihbaratı Portalı, APT tehditleri ve diğer hizmetlere ilişkin analiz raporları sunar ve Bulut Sandbox'a erişim sağlar

Ancak şirketlerin burada yer alan çözümleri ve hizmetleri etkili şekilde kullanabilmesi için uygun deneyim ve uzmanlığa sahip tam gelişmiş bir BT güvenlik departmanı bulundurması gerekir. Şirketlerin bu tür çözüm ve hizmetleri edinmesinin önündeki en temel faktör ise, küresel ölçekte karmaşık tehditlere odaklanmak üzere eğitim alan uzman eksikliği ve bu çalışanları işe almanın maliyetidir.

Patentli bir teknollojiye (patent no. US 10339301B2) sahip Kaspersky Sandbox, kuruluşların sayısı ve karmaşıklığı gideren artan ve mevcut uç nokta korumalarını atlatabilen modern tehditlerle mücadele etmesine yardım eder. Kaspersky Endpoint Security for Business çözümünün işlevselliğini tamamlayan Kaspersky Sandbox, kuruluşların iş istasyonları ve sunucularını daha önceden bilinmeyen kötü amaçlı yazılımlara, yeni virüslere ve fidye yazılımlara, sıfır gün açıklarından yararlanma ve diğer tehditlere karşı sahip olduğu koruma düzeyini, hiçbir yüksek düzeyde uzmanlaşmış bilgi güvenliği analistlerine ihtiyaç duymaksızın yükseltmesine olanak tanır.

Bu sayede küçük işletmeler, yüksek değere sahip uzmanları işe alım harcamalarından tasarruf eder. Aynı zamanda, uzak ofislerindeki etkili bir koruma sağlamak için dağıtılmış ağlara sahip büyük işletmelerin maliyetleri optimize etmesine ve güvenlik analistleri üzerindeki manuel iş yükünü azaltmasına yardımcı olur.

Teslimat ve dağıtım seçenekleri:
Kaspersky Sandbox, bir ISO görüntüsü olarak, önceden yapılandırılmış CentOS 7 ve gerekli tüm çözüm bileşenleri ile birlikte sunulmaktadır. VMware ESXi sistemine bağlı olarak fiziksel bir sunucuya veya sanal sunuculara dağıtılabilmektedir.

Entegrasyon:
- SIEM sistemleri, Kaspersky Sandbox tarafından yapılan tespitlere ilişkin bilgileri alabilir. Bu bilgiler, genel etkinlik akışı içerisinde Kaspersky Security Center üzerinden gönderilir.
- Kaspersky Sandbox ile diğer çözümlerin entegrasyonu için bir API kullanılmaktadır, bu sayede Kaspersky Sandbox çözümünün gönderilecek dosyaların taranması ve talep edilecek dosya geçmişlerinin alınması sağlanır.

Ölçeklenebilirlik
Temel yapılandırma 1000 uç noktaya kadar destekler ve sunmuş olduğumuz çözüm kolay şekilde ölçeklendirilerek büyük altyapılar için sürekli koruma sunar

Kümeleme
Daha fazla kapasite ve yüksek düzeyde bulunurluk için birden fazla sunucu kümelenebilir.

Lisanslama
Kaspersky Sandbox bir yazılım gereci olarak lisanslanır. Bir lisans, 1000 Kaspersky Endpoint Security for Business kullanıcısını desteklemektedir.

Nasıl çalışır?

Karmaşık tehditlerle ve APT seviyesi saldırılarıyla mücadelede en iyi yöntemlerimizi sahip olan Kaspersky Sandbox, Kaspersky Endpoint Security for Business ile ileri düzeyde entegredir. Birleştirilmiş politika tabanlı yönetim konsolumuz olan Kaspersky Security Center üzerinden yönetilmektedir.

Kaspersky Endpoint Security for Business aracısı, Kaspersky Sandbox sunucusunda yer alan ve paylaşımdaki operasyonel karar önbelleğindeki şüpheli bir nesne hakkında veri talebinde bulunur. Nesne daha önce taranmışsa, karar Kaspersky Endpoint Security for Business çözümüne ulaşır ve aşağıdaki seçeneklerden biri veya birkaçı uygulanır:

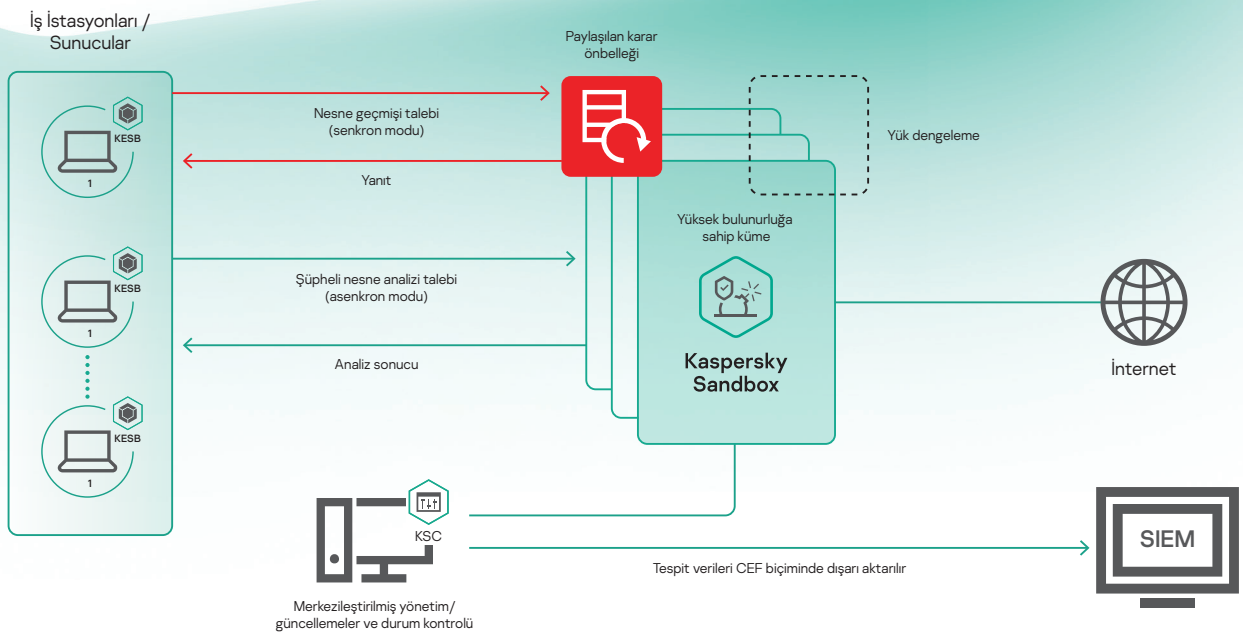
- Kaldır ve karantinaya al
- Kullanıcıya bildir
- Kritik alanlar taraması başlat
- Yönetilen ağ içerisinde bulunan diğer makinelerde tespit edilen nesneyi ara

Nesnenin geçmişine ilişkin karar önbellekten alınamadığında, Kaspersky Endpoint Security for Business aracısı şüpheli dosyayı Sandbox'a gönderir ve yanıt almayı bekler. Nesnenin taranması Sandbox'a ulaşır, test nesnesi gerçek altyapıdan uzak ve izole bir ortamde çalıştırılır.

Dosya tarama işlemi, tipik bir çalışma ortamını (çalışan sistemler/yüklü uygulamalar) taklit eden araçlara sahip sanal makineler içerisinde yapılmaktadır. Nesnedeki kötü amaçlı yazılımı tespit edebilmek adına davranış analizi gerçekleştirilir, yapıtlar toplanır ve analiz edilir; nesnenin kötü amaçlı yazılım eylemleri gerçekleştirmesi halinde Sandbox bu nesneyi kötü amaçlı yazılım olarak tanımlar. Sandbox analizi esnasında, nesneye bir karar atanır.

Nesne benzetim işlemi tamamlandığında, sonuçlanan karar gerçek zamanlı olarak paylaşılan operasyonel karar önbelleğine gönderilir ve bu sayede Kaspersky Endpoint Security for Business yüklü diğer ana bilgisayarların da aynı dosyayı tekrar taramasına gerek kalmadan taranan nesnenin geçmişine ilişkin verileri hızlı şekilde alması sağlanır. Bu yaklaşım sayesinde şüpheli nesnelerin hızlı şekilde işlenmesi sağlanır, Kaspersky Sandbox sunucuları üzerindeki yük azaltılır ve tehditlere verilen yanıtların hızı ve verimliliği iyileştirilir.

Kaspersky Sandbox, Kaspersky Endpoint Security for Business çözümü için oldukça önemli bir eklentidir. Gelişmiş, bilinmeyen ve karmaşık tehditleri ek kaynağa ihtiyaç duymadan otomatik olarak engeller ve BT güvenlik analistlerinin diğer görevlere odaklanabilmesine izin verir.



* Bilgi Güvenliği Tehdit ve Olay Yönetimi

Siber Tehdit Haberleri: www.securelist.com
BT Güvenlik Haberleri: business.kaspersky.com
KOBİ'ler için BT Güvenliği: kaspersky.com.tr/business
Kurumsal BT Güvenliği: kaspersky.com.tr/enterprise

www.kaspersky.com.tr

Başarımız kanıtlanmıştır. Bağımsızız. Şeffafız. Kendimizi teknolojinin hayatlarımızı geliştirdiği daha güvenli bir dünya inşa etmeye adadık. Bu yüzden teknolojiyi güvenli hale getiriyoruz ve böylelikle sunduğu sayısız fırsatlardan herkesin her yerde faydalanmasına katkıda bulunuyoruz. Daha güvenli yarınlar için siber güvenliği yakalayın.

Daha fazla bilgi için: kaspersky.com.tr/transparency

Proven. Transparent. Independent.