Kaspersky Network Security Threat Data Feeds

kaspersky geleceği yakalayın

Uç nokta koruması tek başına yeterli değildir.

Ağ düzeyinde koruma da gereklidir.

Nedenleri:

- Farklı saldırı türlerine karşı koruma birden fazla katmandan oluşmalıdır
- Örneğin, tüm iş açısından kritik sunucular veya endüstriyel bir ağdaki ana bilgisayarlar gibi, ortamınızdaki tüm ana bilgisayarlar uç nokta güvenlik korumasına sahip olmayabilir
- Bazı 'korumalı' ana bilgisayarlar imzala/karmalar/ tespit kuralları ile güncel olmayabilir

Kaspersky Network Security Threat Data Feeds

Bugünlerde neredeyse her şirketin bir Yeni Nesil Güvenlik Duvarı (NGFW) vardır. Kurumsal ağların siber saldırılara karşı koruma seviyelerini artıran en etkili modern ağ güvenliği denetimlerinden biridir.

NGFW'lerin çoğu yalnızca siber tehditler hakkındaki şirket içi bilgileri kullanmakla kalmaz, aynı zamanda siber tehditleri gerçek zamanlı olarak engellemek için dış kaynaklardan gelen dinamik uzlaşma göstergeleri (IoC'ler) listelerini kullanmanıza olanak tanıyan işlevler de sunar

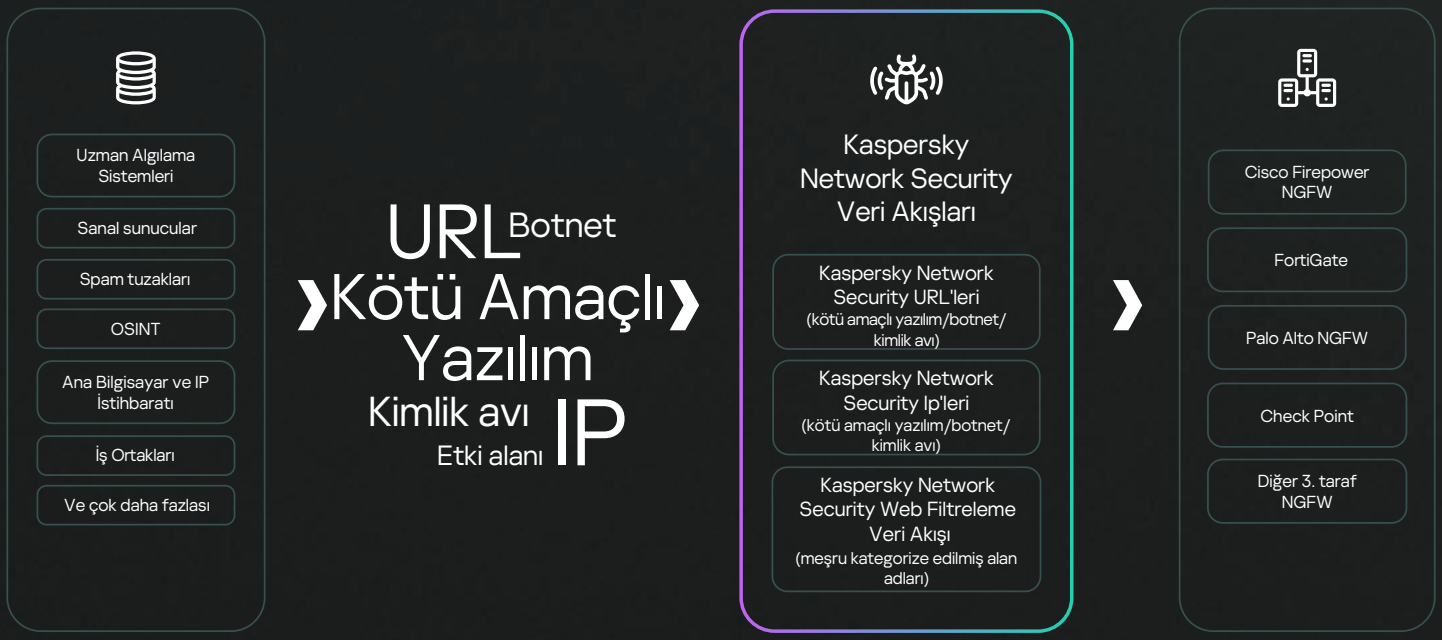
NGFW algılama kurallarını her zaman rakiplerin önünde olacak şekilde hızlıca yapılandırmak neredeyse imkansızdır. Bu nedenle dış tehdit istihbarat bilgisi büyük önem taşır. Ortamınıza, başka türlü gözden kaçabilecek kritik bir ekstra koruma unsuru getirir.

Kaspersky, bir NGFW'ye aktarıldığında, karmaşık entegrasyon veya yapılandırma olmadan ve mevcut ağ topolojisini koruyarak kurumsal ağın en yaygın tehditlere karşı güvenlik koruma düzeyini önemli ölçüde artıran özel olarak oluşturulmuş IoC koleksiyonları sunar.

Kaspersky Network Security Threat Data Feeds, Kaspersky Threat Intelligence Veri Akışlarını temel alır ve çeşitli IoC türlerinin (IP adresleri ve etki alanları) düzenli olarak güncellenen listelerini içerir. Bu bilgileri kullanarak tehlikeli ağ kaynaklarına kullanıcı erişimini izleyebilir/ engelleyebilirsiniz.

Daha fazla bilgi edinin

Kaspersky Network Security Veri Akışları Entegrasyonu



Veri toplama ve işleme

Kaspersky Network Security Veri Akışları, her biri belirli bir siber tehdit türüne odaklanan birden fazla listeden oluşur. Akışlar, en yüksek tehdit puanına sahip IP adreslerinin listelerini ve kötü amaçlı yazılım dağıttığı, botnet komuta ve kontrol merkezleri (C&C) olarak hareket ettiği veya kimlik avı kaynaklarını barındırdığı bilinen kaynakların üst düzey ve ikinci düzey etki alanlarını içerir.

Veri Akışları, Kaspersky Security Network ve proaktif web tarayıcılarımız, Botnet İzleme hizmetimiz (botnetlerin, hedeflerinin ve etkinliklerinin 365 gün 7/24 izlenmesi), ana bilgisayar ve IP istihbarat hizmetleri gibi birleştirilmiş, heterojen ve güvenilir kaynaklardan toplanır.

Toplanan tüm veriler, gerçek zamanlı olarak dikkatlice incelenir ve istatistiksel ölçütler, koruma alanları, sezgisel motorlar, benzerlik araçları, davranış profili çıkarma, analiz ekibi doğrulaması ve izin verilenler listesi doğrulaması gibi birden fazla yeniden işleme tekniği kullanılarak iyileştirilir.

Öne Çıkan Noktalar

Gerçek zamanlı güncellemeler

Veri Akışları, dünya genelindeki bulgulara dayalı şekilde gerçek zamanlı olarak otomatik olarak oluşturulur ve yüksek algılama oranları ve doğruluk seviyeleri sağlar.

Kaspersky Security Network, 213'ten fazla ülkede on milyonlarca son kullanıcıyı kapsayan tüm internet trafiğinin önemli bir yüzdesine görünürlük sağlar

Yerel destek

En popüler NGFW'ler için yerel destek:

- Cisco
- FortiGate
- Palo Alto
- Diğer üçüncü taraf NGFW'ler (temel kimlik doğrulama desteğine sahip harici dinamik listelerin işlevselliği ile)

Güvenli kimlik doğrulama

Veri Akışları, farklı güvenlik ihtiyaçlarını ve entegrasyon tercihlerini karşılamak üzere uyarlanmış çeşitli kimlik doğrulama yöntemleri sunar

Kolay entegrasyon

Desteklenen her NGFW için tamamlayıcı adım adım yapılandırma kılavuzları ve Kaspersky'den teknik destek, kolay yapılandırma sağlar ve anında değer sunar

Sürekli kullanılabilirlik

Tüm akışlar, sürekli kullanılabilirlik sağlayan, hataya yüksek ölçüde dayanıklı bir altyapı tarafından oluşturulur ve izlenir

100% doğrulanmış veriler

Yanlış pozitiflerle dolu Veri Akışları, yasal kaynakları engelleyebileceğinden zararlıdır.

Kaspersky Network Security Veri Akışları, akışları yayınlamadan önce kapsamlı testler ve filtreler uygulayarak %100 doğrulanmış verilerin iletilmesini sağlar

Avantajlar

Ağ savunma çözümlerinizi güçlendirin

en yaygın siber tehditleri otomatik olarak engellemek için sürekli güncellenen IOC'leri kullanın

Hassas varlıkların ve fikri mülkiyetin

virüslü makinelerden kurumunuzun dışına sızmasını önleyin

Kurumunuzu siber tehditlere karşı koruyun

ve iş sürekliliğini sağlamak için siber tehditleri hızla engelleyin

Kaspersky Threat Data Feeds

Daha fazla bilgi edinin

www.kaspersky.com.tr

#kaspersky
#geleceğiyakalayın