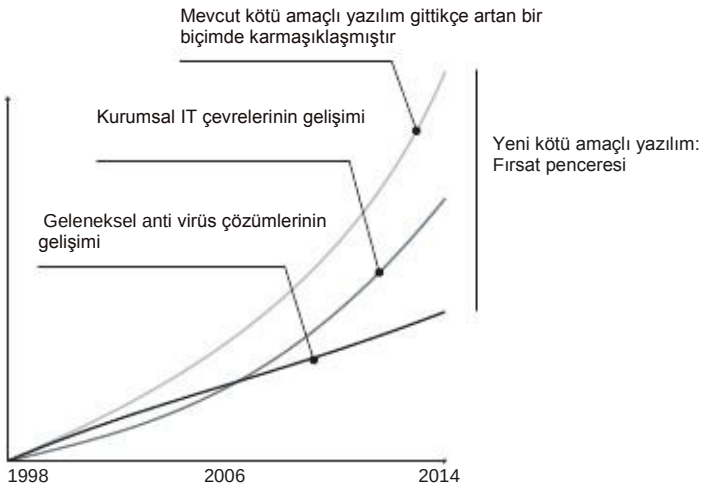
Uyarlanabilir Koruma

Gelişmiş tehditlere karşı fırsat pencerelerini kapatın

ORGANİZASYONUNUZUN SIFIR GÜN SALDIRILARINA VE HEDEFLİ SALDIRILARA KARŞI KORUNDUĞUNU DÜŞÜNÜYOR MUSUNUZ?

Kötü amaçlı yazılım ve IT güvenlik panoraması hacim ve kapsamlılık bağlamında köklü bir değişikliğe gitmiştir. Sirkülâsyondaki virüslerin (yaklaşık 200,000 yeni virüs her gün ortaya çıkmaktadır) sayısında artış olmuştur ve korumaların içine girmeye izin veren ve kötü amaçlı yazılımları saklayan teknikler tehditlerin uzun süre boyunca kurumsal ağlarda kalmalarına olanak sağlamaktadır.



Aynı zamanda, IT çevreleri oldukça karmaşık bir hale gelmiştir, bu da yönetimi daha zor ve sistemleri daha korumasız bir hale getirmiştir.

Geleneksel anti virüs çözümleri gerçeğe henüz ayak uyduramamaktadırlar. Linear gelişimleri, tarihi geçmiş virüs bulma tekniklerini kullanmaya devam etmektedir. Bu teknikler, imza dosyaları ve bulgusal algoritmalar temellidir. Bu da sonuçların doğru olmadığı anlamına gelmektedir. Yani, kötü amaçlı yazılım tespit edilemeyebilir ve yanlış pozitifler üretilebilir.

Bu çelişki, **'kötü amaçlı yazılımlar için fırsat penceresi'** olarak adlandırılan duruma neden olmuştur: yeni virüs ortaya çıkışı ve güvenlik şirketlerinin tedaviyi piyasaya sürmeleri arasındaki süre. Virüs, fidye yazılım, trojanlar ve diğer tip kötü amaçlı yazılımları almak için hackerlar tarafından keşfedilen büyüyen bir boşluk vardır. Bu gelişen tehditler gizli belgelerin şifrelerini çözebilir ve fidye istenebilir veya basitçe endüstriyel casusluk için hassas veri toplayabilir.

Hükümetler, bankalar ve diğer büyük şirketler, geleneksel anti virüs programlarının zamanında belirleyemediği saldırıların hedefi olmaktadır.

Araştırma Bölümümüz, milyonlarca virüs örneğini ve pazardaki en iyi anti virüs programlarını analiz etmişlerdir. Program piyasa çıktığı ilk 24 saat içinde yüzde 18 kötü amaçlı yazılım belirlenmemiş haldedir. Hatta 3 ay sonrasında bile bu geleneksel çözümler kötü amaçlı yazılımların yüzde 2'sini belirleyememektedir.

Bu durumun çözümü **Uyarlanabilir Korumadır**: Meşru olan programların çalışmasına izin veren, organizasyonunuzda çalışan tüm uygulamaları doğru olarak sınıflandıran Panda Güvenlik servisi.

Bunu elde etmek için, beş yıldır üç amaç temeli bulunan **yeni bir güvenlik modeli** üzerinde çalışmaktayız: şirketin bilgisayarları ve serverları üzerindeki uygulamaların sürekli izlenmesi, bulut içindeki Büyük Veri platformumuz üzerinde otomatik öğrenme kullanarak sınıflandırma ve son olarak teknik uzmanlarımız şirket sistemlerinde çalışan her şeyin hareketinden emin olmak için otomatik olarak sınıflandırılmamış uygulamaları analiz eder.

KORUMA
Gelecekteki saldırıları önlemek için uygulamaları engellemek ve sistemleri izole etmek

GÖRÜNÜRLÜK
Çalışan uygulamalarla alınan tüm aksiyonların izlenebilirliği ve görünürlüğü

CEVAP
Her bir denenen saldırı için derin analiz amaçlı hukuki bilgi

BELİRLEME
Hedefli ve sıfır gün saldırıları imza dosyaları olmadan gerçek zamanda engellenmiştir.

TÜM ÇALIŞAN UYGULAMALARIN GÜVENLİĞİNİ GARANTİ ETMEK İÇİN TEK ÇÖZÜM

TAM VE DAYANIKLI KORUMA GARANTİLİ

Panda Uyarlanabilir Korumalar iki operasyonel mod sunar:

• **Standart mod** tüm uygulamaların, Panda Güvenlik ve otomatik sistemlerce kataloglanmış uygulamalarla birlikte, iyi amaçlı yazılım olarak çalışmasına **izin verir.**

• **Genişletilmiş mod sadece** iyi amaçlı yazılımların çalışmasına **izin verir**. Bu, sıfır risk güvenlik yaklaşımı olan şirketler için en uygun koruma şeklidir.

HUKUKİ BİLGİ

• **Uygulama grafikleri** kötü amaçlı yazılımlar yüzünden meydana gelen tüm olaylar hakkında açık bir grafik sunar.

• Kötü amaçlı yazılım bağlantıları, oluşturulan dosyalar ve daha fazlası bağlamında coğrafi kaynaklar üzerindeki **ısı haritaları** aracılığı ile görsel bilgi edinmek.

• Ağınıza kurulmuş bilinen zayıf noktalarla yazılımı yerleştirmek.

GELENEKSEL ANTİ VİRÜS ÇÖZÜMLERİ İLE UYUMLU

Uyarlanabilir Koruma geleneksel anti virüs çözümleri ile bir arada olabilir ve geleneksel çözümlerin belirleyemediği **hedefli ve sıfır gün saldırıları da dahil olmak üzere tüm kötü amaçlı yazılım tiplerini engelleyebilecek kurumsal bir araç rolü** üstlenebilir.

KORUMASIZ İŞLETME SİSTEMLERİ VE UYGULAMALARI İÇİN KORUMA

Geliştiricisi tarafından desteklenmeyen ve bu yüzden korumasız olan Windows XP gibi sistemler sıfır gün ve yeni jenerasyon saldırılar için kolay av durumunda olmaktadırlar.

Üstelik Java, Adobe, Microsoft Office ve tarayıcılar gibi uygulamalardaki zayıflıklar %90 oranında kötü amaçlı yazılımlarca sömürülmektedir.

Uyarlanabilir Koruma modülündeki hassasiyet koruması şirketlerin güncellenmemiş sistemleri olsa bile güvenli bir çevrede çalışmaları için bağlamsal ve davranışsal kurallar kullanmaktadır.

AĞ DURUMUNDA SÜREKLİ BİLGİ

• Ağ üzerinde kötü amaçlı yazılım belirlendiği an uyarı alınır, yer hakkında detaylı bilgi, etkilenen bilgisayarlar ve kötü amaçlı yazılımca alınan aksiyon hakkında geniş kapsamlı bir rapor da beraberinde verilir.

• Hizmetin günlük faaliyeti hakkında e-posta aracılığı ile rapor alınır.

SIEM MEVCUTTUR

Uyarlanabilir Koruma SIEM çözümleri ile bütünleşir ve sistemlerinizde çalışan tüm uygulamaların faaliyetleri hakkında detaylı veri sağlar.

SIEM olmayan müşterilerde, **Uyarlanabilir Koruma** gerçek zamanda toplanmış tüm bilgileri analiz etmek için güvenlik depolaması ve yönetmesi adına kendi sistemlerini içermektedir.

%100 YÖNETİLEN SERVİSLER

Karantina veya şüpheli dosyalarla uğraşmak veya etkilenen bilgisayarları dezenfekte etmek veya iyileştirmek için teknik personele yatırım yapmayı unutun. **Uyarlanabilir Koruma,** PandaLab uzmanlarının sürekli denetimi altındaki büyük veri çevresi içindeki otomatik öğrenme sayesinde tüm uygulamaları otomatik olarak sınıflandırır.

TEKNİK GEREKLİLİKLER

Web Konsolu (sadece izleme)

- İnternet bağlantısı

- İnternet Explorer 7.0 veya daha sonraki sürümleri
- Firefox 3.0 veya daha sonraki sürümleri
- Google Chrome 2.0 veya daha sonraki sürümleri

Araç

- İşletme sistemi (çalışma istasyonları): Windows XP SP2 ve daha sonraki sürümler, Vista, Windows7,8 & 8.1

- İşletme sistemleri (serverlar): Windows 2003 Server, Windows 2008, Windows Server 2012

- İnternet bağlantısı (doğrudan veya Proxy ile)