SOPHOS
Security made simple.

Intercept X

Derin öğrenme teknolojisi ile kötü niyetli yazılımların tespit edilmesi, Exploit Prevention, Fidye yazılımı önleme, Kök neden analizi ve Sophos Clean

Sophos Intercept X bilinmeyen saldırıları durdurmak ve saldırganı önlemek için doğru tekniği doğru zamanda kullanır. Mevcut kullandığınız Antivirüs yazılımı ile birlikte yada Sophos Endpoint Protection antivirus yazılımı ile birlikte kullanabileceğiniz yeni nesil katmanlı koruma teknolojisidir.

Öne Çıkan Noktalar

- Eğitimli derin öğrenme modelleri görülmeyen kötü amaçlı yazılımları saptar
- Exploit Prevention saldırganların savunmasız yazılımı kontrol etmede kullandığı teknikleri işlevsiz kılar
- Oluşabilecek çeşitli zaafiyetlere karşı sisteminizin istismar edilmesini kalıcı olarak önler.
- Kök neden analizi kötü amaçlı yazılımın neler yaptığını ve nereden geldiğini görmenizi sağlar
- Sophos Clean kötü amaçlı yazılımları ve geri kalan kalıntıları temizler
- Var olan antivirüs yatırımınızın etkinliğini artırır

Yeni nesil uç nokta koruma güvenliğinizi inşa edin

Basit dosya tarama yöntemleri çoktan geride kaldı. Amacınız artık tehditlerin bilgisayarınıza erişmesini engellemek, onları çalışmadan önce durdurmak, önleyici yöntemleri geçmişler ise onları saptamak ve kötü amaçlı yazılımı yalnızca silmek yerine analiz etmek ve yaptıkları her şeyi geri almaktır.

Sophos Intercept X tam anlamıyla yeni nesil uç nokta güvenli sağlamak için mevcut antivirus yazılımınızda bulunan çok katmanlı teknolojiyi kullanır.

Derin Ögrenme Teknolojisi ile Kötü Niyetli Yazılımların Tespit Edilmesi

Derin Ögrenme Sinir Ağları ile SophosLabs ortamında eğitilen Intercept X yeni ve sıfırıncı gün zararlı yazılımları yüksek doğruluk oranı ile herhangi bir imza veritabanı kullanmadan tespit eder. Makine öğreniminin alternatif yöntemleri genellikle veri bilimcilerinin aranacak öznitelikleri tanımlamasını gerektirir. Dolayısıyla nihai model bu öznitelik seçiminin ve eğitim verisinin verimliliği açısından kısıtlanmıştır. Intercept X'te kullanılan derin öğrenme, kendisi için kötü amaçlı yazılım ile zararsız dosyaları birbirinden ayırmak için önemli öznitelikleri belirler. Bu, SophosLabs'in sunduğu kapsamlı eğitim verileri ile birleşerek zararsız ve kötü amaçlı dosyalar arasında doğru ve etkin bir karar sınırı oluşturur. Bu eğitilmiş model boyutta 20 mb'tan daha küçüktür ve az sıklıkta güncelleştirme gerektirir. Buluta dönüldüğünde ise, SophosLabs modeli sürekli olarak eğitmekte, yeni ve eski kötü amaçlı yazılım örneklerini kullanarak karar sınırının etkinliğini gözlemlemektedir.

Savunmasız yazılımlarınızı koruyun

Güvenlik açıkları alarm verici bir hızda artmaktadır. Bunlar yazılımdaki eksiklikleri temsil eder ve satıcılar tarafından düzeltilmelidir. Öte yandan yeni exploit teknikleri yılda ortalama olarak yalnızca iki kez ortaya çıkar ve saldırganlar tarafından keşfedilen her güvenlik açığında tekrar tekrar kullanılır. Exploit Prevention, güvenlik açığı düzeltilmeden önce saldırganların bu açıktan faydalanmalarına engel olur. Yani, bu teknikleri işlevsiz kılar.

Etkin fidye yazılımı saptaması

CryptoGuard teknolojisi rastgele kötü amaçlı veri şifrelemesini saptayarak fidye yazılımlarını iş üstünde yakalar. Güvenilir dosyalarınız ele geçirilmiş veya zarar görmüş olsa bile, CryptoGuard bunları durdurur ve kullanıcılarla veya BT destek personeliyle herhangi bir etkileşimleri olmaksızın etkisiz hale getirir. CryptoGuard, uzaktaki bilgisayarları ve yerel prosesleri değiştirmeye çalışan işlemleri takip ederek dosya sistemi seviyesinde sessizce çalışır.

Kök neden analizi

Kötü amaçlı yazılımı saptamak ve kaldırmak problemi geçici olarak çözer. Fakat kötü amaçlı yazılımın kaldırılmadan önce ne yaptığını veya ilk etapta sisteminize nasıl bulaştığını gerçekten biliyor musunuz? Kök neden analizi saldırıyı saptamayla sonuçlanan tüm olayları gösterir. Kötü amaçlı yazılımların hangi dosyalara, işlemlere ve kayıt defteri anahtarlarına etki ettiğini anlayabilir ve sistemi eski haline getirmek için zamanı geri sarabilir.

Yönetimi ve kurulumu basitleştirin

Güvenliğinizi Sophos Central'dan yönetmek, uç noktalarınızı güvence altına almak için sunucuların kurulmasına ve çalıştırılmasına gerek kalmadığı anlamına gelir. Sophos Central, ilk günden itibaren en etkili korumayı edinmenizi sağlamak için varsayılan politikaları ve önerilen konfigürasyonları sağlar.

	Özellikler	
EXPLOIT PREVENTION	Veri Yürütme Engellemesi Zorlama	✓
	Zorunlu ASLR	✓
	Aşağıdan Yukarıya ASLR	✓
	Null Sayfa (Null Riayet Koruması)	✓
	Heap Spray Ayırma	✓
	Dinamik Heap Spray	✓
	Yığın Özeti	✓
	Yığın Yürütme (MemProt)	✓
	Yığın Tabanlı ROP Azaltmaları (Arayan)	✓
	Dal Tabanlı ROP Azaltmaları (Donanım Destekli)	✓
	Yapılandırılmış Özel Durum İşleme Üzerine Yazma Koruması (SEHOP)	✓
	Import Address Table Filtreleme (IAF)	✓
	Load Library	✓
	Reflective DLL Injection	✓
	Kabuk Kodu	✓
	VBScript God Mode	✓
	Wow64	✓
	Sistem Çağrısı	✓
	Hollow Process	✓
	DLL Hijacking	✓
	Squiblydoo Applocker Bypass	✓
	APC Koruması (Double Pulsar / AtomBombing)	✓
	Yetki Yükseltme Prosesi	✓
AKTİF DÜŞMAN AZALTMALARI	Kimlik Hırsızlığı Koruması	✓
	Code Cave Azaltımı	✓
	Man-in-the-Browser Koruması (Güvenli tarama)	✓
	Kötü Amaçlı Trafik Saptama	✓
	Meterpreter Kabuk Saptama	✓

Yönetim için zaten Enterprise Console'lu Sophos Endpoint Protection mı kullanıyorsunuz? Uç noktalarınızı Sophos Central kullanarak ve Intercept X'i otomatik çalışmak üzere etkinleştirerek yönetebilirsiniz.

Korumanın dört adımı

1. Deneme sürümünüzü başlatmak için sophos.com/intercept-x adresini ziyaret edin.
2. Sophos Central sistem yöneticisi hesabı oluşturun.
3. Intercept X birimini indirin ve yükleyin.
4. Korumanızı Sophos Central üzerinden yönetin.

Teknik gereksinimler

Sophos Intercept X, Windows 7 ve üzeri, 32 ve 64 bit sistemleri destekler. Sophos Central tarafından yönetildiğinde Endpoint Protection Standard veya Advanced'in yanında çalışabilir. Ayrıca derin öğrenme kötü amaçlı yazılım saptaması, exploit önleme, fidye yazılımı önleme, kök neden analizi ve Sophos Clean'e katkıda bulunmak üzere üçüncü tarafların uç nokta koruması ve antivirüs programlarıyla birlikte de çalışabilir.

	Özellikler	
FİDYE YAZILIMI ÖNLEME	Fidye Yazılımı Dosyası Koruması (CryptoGuard)	✓
	Otomatik Dosya Onarma (CryptoGuard)	✓
	Disk ve Ön Yükleme Kaydı Koruması (WipeGuard)	✓
UYGULAMA KİLİTLEME	Web Tarayıcıları (HTA dahil)	✓
	Web Tarayıcı Eklentileri	✓
	Java	✓
	Ortam Uygulamaları	✓
	Ofis Uygulamaları	✓
DERİN ÖĞRENME	Derin Öğrenme Kötü Amaçlı Yazılım Saptaması	✓
	Derin Öğrenme Potansiyel İstenmeyen Uygulama (PUA) Engelleme	✓
	Yalancı pozitiflik yok etme	✓
	Canlı Koruma	✓
REAKSİYON SORGULAMA KALDIRMA	Kök Neden Analizi	✓
	Sophos Clean	✓
	Senkronize Security Heartbeat	✓
KURMA	Bağımsız birim olarak çalışabilir	✓
	Mevcut antivirüs programı ile birlikte çalışabilir	✓
	Mevcut Sophos Endpoint biriminin bileşeni olarak çalışabilir	✓
	Windows 7	✓
	Windows 8	✓
	Windows 8.1	✓
	Windows 10	✓
	macOS*	✓

* CryptoGuard, Kötü Amaçlı Trafik Saptama, Senkronize Security Heartbeat, Kök Neden Analizi özelliklerini destekler

Şimdi ücretsiz deneyin

Ücretsiz 30 günlük değerlendirmeye sophos.com/intercept-x adresinde kaydolun.

Palladium Ofis ve Residence Binasi,
Barbaros Mahallesi Halk Caddesi No:8/A Kat:2-3,
Ataşehir, 34746 İstanbul
+90 216 663 61 61
salesmea@sophos.com

2018-04-10-DS-TR (PC)

SOPHOS