SOPHOS

Intercept X

Rakipsiz Endpoint Koruması

Sophos Intercept X, derin öğrenimli zararlı yazılım tespiti, suistimallere karşı koruma, fidye yazılımlarına karşı modülleri ve daha bir çok özelliğiyle en geniş yelpazede koruma sağlar.

Öne Çıkan Özellikler

- Derin öğrenimle birlikte #1 numaralı zararlı yazılım tespit motoru
- Suistimal önleme, saldırganın açığı olan yazılımdan faydalanmasını önleme
- Etkin zararlı azaltma özelliği cihaza yönelik yapılan sürekli saldırıları önler
- Kök neden analizi, zararlı yazılımın neler yaptığını ve nereden geldiğini gösterir
- Fidye yazılımı önleyici teknoloji
- Intercept X mevcut antivirüs uygulamanızı daha da etkili hale getirir. Intercept X Advanced geleneksel metodlar kullanan endpoint güvenliğinize modern teknikler ekler

Sophos Intercept X, tek bir güvenlik yöntemiyle yetinmeyerek endpoint koruması için bütünleşik derin defans ilkesini benimsemiştir. Bu ilke üzerinden geleneksel güvenlik metodlarının yanında modern teknikleri bir çatıda birleştirmiştir.

Bu modern teknikler: derin öğrenimli zararlı yazılım tespiti, suistimal önleme ve fidye yazılımlarına karşı çözümleri de içerir. Bünyesinde barındırdığı temel özellikler arasında ise imza tabanlı zararlı yazılım tespiti, davranış analizi, zararlı veri trafiği tespiti, cihaz denetleme, uygulama denetleme, web filtreleme, veri kaybı önleme ve daha bir çok araç bulunmaktadır.

Derin Öğrenimli Zararlı Yazılım Tespiti

Intercept X içinde bulunan yapay zeka, derin öğrenimli nöral bir ağdır, aynı zamanda bilinen ve bilinmeyen zararlı yazılımları tespit eden makine öğreniminin ileri bir düzeyidir.

Derin öğrenim ile güçlendirilmiş olan Intercept X, üçüncü parti kurumlarca onaylandığı üzere sektöründe var olan en iyi zararlı yazılım tespit motorudur. Bu özellikleriyle Intercept X, diğer antivirüs üreticilerinin kaçırdığı zararlı yazılımları yakalar.

Suistimali ve Saldırıları Önleyin

Yazılımlarda bulunan açıklar endişe verecek hızda bulunmakta ve üreticilerin bu açıkları sürekli olarak kapatması gerekmektedir. Yeni suistimal teknikleri ender olmakla beraber, saldırganların bu teknikleri sürekli olarak yeni yazılımlarda kullandığı görülmektedir.

Suistimale karşı koruma, saldırganların zararlı yazılım dağıtımı, kullanıcı bilgilerinin çalınması için kullanılan suistimal araçlarını ve tekniklerini engelleyerek önler. Bu teknoloji ile Sophos'tan bu tip saldırılar kaçmaz ve sıfır günlerine karşı da korunur olursunuz.

Onaylı Fidye Yazılım Koruması

Intercept X, daha önceden karşılaşılmamış fidye yazılımı ve önyükleme kaydı yapan saldırılara karşı davranışsal analiz kullanarak varolan en iyi fidye yazılım karşıtı çözümünü kullanmaktadır. Güvenilir dosya ve işlemler dahi suistimal edilebilmekte ve hacklenebilmektedir. CryptoGuard bu gibi durumları önler ve kullanıcı veyahut sistem yöneticisinden bağımsız olarak bu tip saldırılardan korur. CryptoGuard dosya sistem seviyesinde sessizce çalışır, lokalde bulunan işlemler ve uzak lokasyonda bulunan bilgisayarlar üzerinde değişiklik yapma girişimlerini takip eder.

Endpoint Tespit ve Müdahale (EDR)

Endpoint tespit ve müdahale özelliği, konvansiyonel tehditlerin yanında ilave tehditleri tespit, derinlemesine denetim ve müdahale için gereklidir. Sophos Intercept X Advanced with EDR, türünün en iyisi olan endpoint koruması ile entegre olarak tek bir çatıda çözüm sunar. Bu sayede işletmeler güvenlik vakalarıyla ilgili olan zor problemleri çözer.

Basit Yönetim ve Kurulum

Sophos Central üzerinden yönetim sayesinde herhangi bir sunucuya yükleme yapmanıza gerek kalmaz. Sophos Central, size ilk günden varsayılan kurallar ve tavsiye edilen yapılandırmasıyla etkin bir koruma sağlar.

Tehdit Müdahale Yönetimi (MTR)

Sophos uzmanları tarafından yönetilen bir hizmet olarak 7/24 tehdit avı, tespit ve müdahale sağlar. Intercept X Advanced with EDR içinde bulunan istihbarat özelliği ile, Sophos uzmanları potansiyel tehditlere yanıt verir, sorunun nereden kaynaklandığını bulur, vakaların nerede, ne zaman, nasıl ve neden oluştuğuna dair detaylı analiz sunar.

Teknik Özellikler

Sophos Intercept X, 32 ve 64 bit olan Windows 7 ve daha yeni işletim sistemlerini desteklemektedir. Aynı zamanda üçüncü parti endpoint çözümleriyle de sorunsuzca çalışabilir. Böylece mevcut korumanıza derin öğrenimle zararlı yazılım tespiti, suistimale karşı koruma, fidye yazılımlarına karşı koruma, kök neden analizi ve Sophos Clean teknolojilerinden yararlanabilirsiniz.

	Features	
EXPLOIT PREVENTION	Enforce Data Execution Prevention	✓
	Mandatory Address Space Layout Randomization	✓
	Bottom-up ASLR	✓
	Null Page (Null Deference Protection)	✓
	Heap Spray Allocation	✓
	Dynamic Heap Spray	✓
	Stack Pivot	✓
	Stack Exec (MemProt)	✓
	Stack-based ROP Mitigations (Caller)	✓
	Branch-based ROP Mitigations (Hardware Assisted)	✓
	Structured Exception Handler Overwrite (SEHOP)	✓
	Import Address Table Filtering (IAF)	✓
	Load Library	✓
	Reflective DLL Injection	✓
	Shellcode	✓
	VBScript God Mode	✓
	Wow64	✓
	Syscall	✓
	Hollow Process	✓
	DLL Hijacking	✓
	Squiblydoo Applocker Bypass	✓
	APC Protection (Double Pulsar / AtomBombing)	✓
	Process Privilege Escalation	✓
ACTIVE ADVERSARY MITIGATIONS	Credential Theft Protection	✓
	Code Cave Mitigation	✓
	Man-in-the-Browser Protection (Safe Browsing)	✓
	Malicious Traffic Detection	✓
	Meterpreter Shell Detection	✓

	Features	
ANTI-RANSOMWARE	Ransomware File Protection (CryptoGuard)	✓
	Automatic File Recovery (CryptoGuard)	✓
	Disk and Boot Record Protection (WipeGuard)	✓
APPLICATION LOCKDOWN	Web Browsers (including HTA)	✓
	Web Browser Plugins	✓
	Java	✓
	Media Applications	✓
	Office Applications	✓
DEEP LEARNING	Deep Learning Malware Detection	✓
	Deep Learning Potentially Unwanted Applications (PUA) Blocking	✓
	False Positive Suppression	✓
	Live Protection	✓
RESPOND INVESTIGATE REMOVE	Root Cause Analysis	✓
	Sophos Clean	✓
	Synchronized Security Heartbeat	✓
DEPLOYMENT	Can run as standalone agent	✓
	Can run alongside existing antivirus	✓
	Can run as component of existing Sophos Endpoint agent	✓
	Windows 7	✓
	Windows 8	✓
	Windows 8.1	✓
	Windows 10	✓
	macOS*	✓

*** Features supported include CryptoGuard, Malicious Traffic Detection,Synchronized Security Heartbeat, Root Cause Analysis**

https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/Sophos-Comprehensive-Exploit-Prevention-wpna.pdf

SOPHOS