SOPHOS

Intercept X

Páratlan végpontbiztonság
A Sophos Intercept X gépi tanulással, exploitok elleni védelemmel és zsarolóvírusokkal szemben kifejlesztett funkciókkal állítja meg napjaink legszélesebb körben fenyegető támadásait.

Jellemzők

Kiemelkedő malware detektálás mély tanulással

Exploitok elleni védelem a szoftveres sebezhetőségek kihasználásának megakadályozása érdekében

Aktív támadásblokkolás; képes visszaverni a gép irányításának átvételére tett kísérleteket

Kiváltó okok elemzése a kártékony kódok viselkedésének és forrásának megállapításához

Zsarolóvírusok elleni specializált védelmi technológia

Az Intercept X fokozza a meglévő víruskeresők hatékonyságát. Az Intercept X Advanced pedig kompletten felváltja az eddigi végpontvédelmet a legmodernebb technológiák ötvözésével.

A Sophos Intercept X nem csupán egyetlen biztonsági technológiára fókuszál, hanem mélységi megközelítéssel biztosítja az átfogó végpontvédelmet. A nagyfokú hatékonyság érdekében korszerű, piacvezető megoldásokat egyesít.

A legmodernebb technológiák között megtalálható a mély tanulásra épülő malware detektálás, az exploitok elleni védelem és a zsarolóvírusokkal szemben kifejlesztett célzott védelmi funkciók is. Emellett természetesen a klasszikus alaptechnológiák is helyet kaptak a termékben, mint amilyen a szignatúra alapú vírusvédelem, a viselkedéselemzés, a kártékony adatforgalom detektálása, a csatlakoztatott eszközök felügyelete, az alkalmazás kontroll, a webes tartalomszűrés, vagy az adatszivárgás-megelőzés.

Kártékony programok felismerése gépi tanulással

A mesterséges intelligencia az Intercept X szerves részét képezi. A mély tanulásra és a mély neurális hálózatokra épülő gépi tanulás révén mind az ismert, mind az ismeretlen kártékony kódok szignatúrák nélkül válnak kiszűrhetővé.

A mély tanulással felvértezett Intercept X a piac leghatékonyabb malware detektáló motorját foglalja magában, amit független tesztek is igazolnak. Ennek köszönhetően az Intercept X olyan kártékony programokat is képes kiszűrni, amelyek más végpontbiztonsági eszközökön áthatolnak.

Megfékezett exploitok és támadások

Szoftveres sérülékenységek aggasztó számban vannak jelen. Ugyanakkor biztonsági rések kihasználására alkalmas új technikák jóval ritkábban jelennek meg – a támadók általában az új sérülékenységeket is a meglévő támadási metódussal próbálják kihasználni. Az Intercept X részét képező, exploitok ellen védő funkció pontosan ezeket a vírusterjesztéshez, adatlopáshoz és védelmi mechanizmusok megkerüléséhez is felhasználható technikákat hivatott felismerni, illetve blokkolni – és így a nulladik napi sérülékenység ellen is védelmet nyújtani.

Bizonyított védelem zsarolóvírusok ellen

Az Intercept X viselkedéselemzést is alkalmaz a zsarolóvírusokra épülő vagy a boot szektort manipuláló támadások blokkolásához. Ezáltal az elérhető legfejlettebb anti-ransomware technologiát képviseli. A CryptoGuard megakadályozza a zsarolóvírusok által kezdeményezett műveleteket, miközben az esetlegesen kompromittált állományokat emberi közreműködés nélkül, automatikusan helyreállítja. A CryptoGuard a háttérben észrevétlenül, a fájlrendszer szintjén működik, és detektálja azon támadási kíséreteket, amelyek dokumentumok és egyéb fájlok manipulálására irányulnak.

Végponti detektálás és reagálás (EDR)

A végponti detektálási és reagálási képességek alapvetően szükségesek a további fenyegetettségek detektálásához, az incidensek kivizsgálásához és a magabiztos válaszlépések megtételéhez. A Sophos Intercept X Advanced with EDR egy intelligens EDR-megoldást foglal magában az iparágban magasan rangsorolt végpontvédelmi technológiákkal egyetemben. Ennek köszönhetően a szervezetek a biztonsági incidensek kapcsán kritikus kérdésekre kaphatnak megalapozott válaszokat.

Egyszerű felügyelet és telepítés

A Sophos Centralnak köszönhetően nem kell többé szervereket telepíteni és üzemeltetni a végpontok védelmének biztosításához. A Sophos Central alapértelmezett házirendekkel és legjobb gyakorlatokra épülő konfigurációs beállításokkal segíti a legerősebb védelem kialakítását.

Fenyegetettségek menedzselt kezelése

A Sophos szakértői folyamatosan (24/7) keresik a legújabb fenyegetettségeket, és dolgozzák ki az azok elhárításához szükséges megoldásokat menedzselt szolgáltatás keretében. Az Intercept X Advanced with EDR részeként a Sophos részletes elemzést biztosít a biztonsági eseményekkel kapcsolatban (hol, mi, mikor hogyan és miért történt).

Technikai specifikációk

A Sophos Intercept X támogatja a Windows 7 és az annál újabb operációs rendszereket. Párhuzamosan futtatható más gyártók végpontbiztonsági megoldásaival annak érdekében, hogy azok mély tanulásra épülő malware detektálással, exploitok és zsarolóvírusok elleni védelemmel, valamint mélyszintű elemzési lehetőségekkel legyenek kiegészíthetők.

	Jellemzők	
EXPLOITOK ELLENI VÉDELEM	DEP (Data Execution Prevention) kikényszerítés	✓
	ASLR (Address Space Layout Randomization) ellenőrzés	✓
	ASLR-megkerülés ellenőrzése	✓
	Null Page (Null Deference)	✓
	Heap Spray	✓
	Dynamic Heap Spray	✓
	Stack Pivot	✓
	Stack Exec (MemProt)	✓
	Stack-based ROP	✓
	Branch-based ROP	✓
	Structured Exception Handler Overwrite (SEHOP)	✓
	Import Address Table Filtering (IAF)	✓
	Szoftverkönyvtárak betöltése	✓
	Reflektív DLL-befecskendezés	✓
	Shellcode	✓
	VBScript God Mode	✓
	Wow64	✓
	Rendszerhívások (Syscall)	✓
	Kódbefecskendezés (Hollow Process)	✓
	DLL-hijacking	✓
	Squiblydoo Applocker Bypass	✓
	APC-védelem (Double Pulsar / AtomBombing)	✓
	Jogosultsági szint emelés	✓
AKTÍV TÁMADÁS-BLOKKOLÁS	Hitelesítési adatok eltulajdonításának megelőzése	✓
	Code Cave típusú támadások elhárítása	✓
	Közbeékelődéses támadások elleni védelem	✓
	Kártékony adatforgalom detektálás	✓
	Meterpreter detektálás	✓

	Jellemzők	
ZSAROLÓ-VÍRUSOK ELLENI VÉDELEM	Zsarolóvírusok elleni védelem (CryptoGuard)	✓
	Automatikus fájlhelyreállítás (CryptoGuard)	✓
	Lemez- és boot szektor védelem (WipeGuard)	✓
ALKALMAZÁSOK EREDETISÉGÉN EK VÉDELME	Webböngészők (HTA is)	✓
	Webböngésző bővítmények	✓
	Java	✓
	Média alkalmazások	✓
	Irodai szoftverek	✓
GÉPI TANULÁS	Mély tanulásra épülő malware felismerés	✓
	Nemkívánatos alkalmazások (PUA) blokkolása mély tanulással	✓
	Hamis riasztások számának csökkentése	✓
	Live Protection technológia	✓
VIZSGÁLAT ÉS ELEMZÉS	Kiváltó okok elemzése (Root Cause Analysis)	✓
	Sophos Clean technológia	✓
	Synchronized Security Heartbeat technológia	✓
TELEPÍTÉS	Agent alapú futtatás lehetősége	✓
	Párhuzamos használat meglévő antivírus szoftverrel	✓
	Komponensként történő futtatás Sophos Endpoint agenttel	✓
	Windows 7	✓
	Windows 8	✓
	Windows 8.1	✓
	Windows 10	✓
	macOS*	✓

*Támogatott funkciók: CryptoGuard, kártékony hálózati adatforgalom detektálás, Synchronized Security Heartbeat, gyökér okok elemzése

Már használja a Sophos Endpoint Protection megoldást Enterprise Console-lal?
A végpontok védelmét a Sophos Central segítségével menedzselheti, és engedélyezheti az Intercept X technológiát.

Próbálja ki ingyenesen!

Regisztráljon 30 napos próbaverzióra a sophos.com/intercept-x weboldalon.

Magyarországi disztribútor:
RelNet Technológia Kft.
1047 Budapest, Váci út 71.
Tel: +36 (1) 48 48 300
Email: info@relnet.hu

SOPHOS