SOPHOS
Security made simple.

Intercept X

Détection des malwares grâce à la technologie Deep Learning, prévention des exploits, anti-ransomware, analyse détaillée des attaques (Root cause analysis) et Sophos Clean.

Sophos Intercept X utilise la technologie adéquate au bon moment pour bloquer les menaces inconnues et repousser l'attaque. Il s'utilise en complément de votre antivirus ou de Sophos Endpoint Protection pour une protection Next-Gen complète.

Principaux avantages

- Les modèles alimentés par la technologie Deep Learning détectent les malwares inconnus
- La prévention des exploits bloque les technologies utilisées par les pirates pour contrôler les logiciels vulnérables
- Les mécanismes de défense contre le piratage préviennent la persistance dans la machine
- L'analyse détaillée des attaques (Root cause analysis) vous permet de connaître d'où vient le malware et son impact
- Sophos Clean élimine les malwares et les tous les éléments qui en résultent.
- Complète la protection apportée par votre antivirus actuel.

Renforcez votre sécurité Endpoint Next-Gen

Le temps de l'analyse simple des fichiers est révolu. Votre objectif est désormais d'empêcher les menaces d'atteindre vos systèmes, de les stopper avant qu'elles ne s'exécutent, de les détecter si elles ont contourné les outils de prévention et d'aller au-delà du simple nettoyage de malwares, en analysant et en restaurant tout ce qui a été touché sur vos systèmes. Sophos Intercept X utilise plusieurs couches de technologies qui co-existent avec votre antivirus pour fournir une protection Next-Gen complète.

Détection des malwares grâce à la technologie Deep Learning

Instruit par les SophosLabs via la création de réseaux neuronaux par Deep Learning, Intercept X détecte les fichiers de malwares nouveaux ou inconnus avec une grande précision, sans signatures. Les méthodes alternatives de Deep Learning impliquent souvent que les experts en données identifient les critères à rechercher. Le modèle qui en résulte est alors limité par l'efficacité de la sélection des critères et des données d'apprentissage. La technologie de Deep Learning utilisée dans Intercept X identifie les critères importants pour distinguer les malwares des fichiers inoffensifs. Ceci, associé à un large ensemble de données d'apprentissage fourni par les SophosLabs, garantit la création d'une délimitation précise et efficace entre les fichiers malveillants et les fichiers inoffensifs. Ce modèle d'apprentissage nécessite une taille inférieure à 20mb et des mises à jour espacées. Dans le Cloud, les SophosLabs façonnent le modèle en permanence et surveillent l'efficacité de la délimitation en utilisant des échantillons nouveaux et inconnus.

Protection des logiciels vulnérables

Les vulnérabilités se présentent à un rythme alarmant. Elles représentent des failles dans les logiciels et les éditeurs doivent publier des correctifs pour y remédier. Les nouvelles techniques d'exploits émergent elles en moyenne deux fois par an et sont utilisées de façon répétée par les pirates avec chaque vulnérabilité découverte. La prévention contre les exploits enraye ces techniques, empêchant ainsi le pirate d'exploiter la vulnérabilité avant que le correctif ne soit appliqué.

Détection efficace des ransomwares

La technologie CryptoGuard détecte le chiffrement spontané et malveillant de données, afin de stopper net le ransomware dans son élan. Même si des fichiers ou des processus fiables sont corrompus ou piratés, CryptoGuard les bloquera et les restaurera, le tout sans nécessiter d'intervention de la part de l'utilisateur ou du support informatique. CryptoGuard fonctionne silencieusement au niveau du système de fichiers, surveillant l'activité d'ordinateurs distants et de processus locaux qui tentent de modifier vos documents ou d'autres fichiers.

Analyse détaillée des attaques

Identifier le malware puis l'isoler et le supprimer résout le problème immédiatement. Mais savez-vous réellement ce que le malware a eu le temps de faire avant d'être supprimé? Ou comment il s'est introduit dans vos systèmes ? Le rapport détaillé affiche tous les événements ayant conduits à la détection. Vous serez en mesure de déterminer quels fichiers, quels processus et quelles clés de registre ont été touchés par le malware, et d'activer le nettoyage avancé de votre système pour qu'ils retrouvent leur état initial.

Simplifier la gestion et le déploiement

Gérer votre sécurité depuis Sophos Central signifie que vous n'avez plus besoin d'installer ou de déployer des serveurs pour sécuriser vos systèmes d'extrémité. Sophos Central propose des politiques par défaut et recommande des configurations afin de garantir que vous disposiez de la meilleure protection dès le premier jour.

Protection en quatre étapes

1. Visitez sophos.fr/intercept-x to start your trial.
2. Créez un compte administrateur Sophos Central.
3. Téléchargez et installez l'agent Intercept X.
4. Administrez votre protection via Sophos Central.

Spécifications techniques

Sophos Intercept X prend en charge Windows 7 et supérieur, 32 et 64 bits. Il peut s'exécuter en plus de Sophos Endpoint Protection Standard ou Advanced lorsqu'il est géré par Sophos Central. Il peut également fonctionner en complément de tout autre produit antivirus ou Endpoint tiers, pour apporter d'autres fonctions telles que la technologie Deep Learning, l'anti-exploit, l'anti-ransomware, l'analyse détaillée et Sophos Clean.

	Fonctions	
PREVENTION DES EXPLOITS	Application de la Prévention de l'exécution des données (PED)	✓
	Application systématique de la technique ASLR	✓
	Randomisation du format d'espace d'adresse (ASLR) ascendante	✓
	Protection contre le déréférencement pointeur Null	✓
	Allocation de Heap Spray	✓
	Dynamic Heap Spray	✓
	Stack Pivot	✓
	Stack Exec (MemProt)	✓
	Anti-ROP de la pile (instruction d'appel)	✓
	Anti-ROP du branchement (assisté par matériel)	✓
	Structured Exception Handler Overwrite (SEHOP)	✓
	Filtrage des accès à la table d'import (IAF)	✓
	Chargement de la bibliothèque	✓
	Reflective DLL Injection	✓
	Shellcode	✓
	VBScript God Mode	✓
	Wow64	✓
	Syscall (Appel système)	✓
	Hollow Process	✓
	DLL Hijacking	✓
	Squiblydoo Applocker Bypass	✓
	Protection APC (Double Pulsar / AtomBombing)	✓
	Processus d'élévation des privilèges	✓
MECANISMES DE DEFENSE CONTRE LE PIRATAGE	Protection contre le vol d'identifiants	✓
	Prévention du Code Cave	✓
	Protection MITB (Navigation sécurisée)	✓
	Détection du trafic malveillant	✓
	Détection de Meterpreter Shell	✓

	Fonctions	
ANTI-RANSOMWARE	Protection des fichiers contre les ransomwares (CryptoGuard)	✓
	Récupération automatique de fichiers (CryptoGuard)	✓
	Protection de l'enregistrement de démarrage et du disque (WipeGuard)	✓
VERROUILLAGE DES APPLICATIONS	Navigateurs Web (y compris HTA)	✓
	Plugins navigateurs Web	✓
	Java	✓
	Applications Media	✓
	Applications Office	✓
DEEP LEARNING	Détection des malwares par Deep Learning	✓
	Blocage des applications potentiellement indésirables (PUA) par Deep Learning	✓
	Élimination des faux positifs	✓
	Live Protection	✓
RÉPONSE INVESTIGATION ELIMINATION	Analyse de l'origine de l'attaque	✓
	Sophos Clean	✓
	Synchronized Security Heartbeat	✓
DEPLOIEMENT	Peut s'utiliser comme agent autonome	✓
	Peut s'utiliser en complément de l'antivirus existant	✓
	Peut s'utiliser comme composant d'un agent Sophos Endpoint existant	✓
	Windows 7	✓
	Windows 8	✓
	Windows 8.1	✓
	Windows 10	✓
	macOS*	✓

* fonctions prises en charge CryptoGuard, Détecteur du trafic malveillant, Synchronized Security Heartbeat, Root Cause Analysis

Vous utilisez Enterprise Console pour gérer Sophos Endpoint Protection ? Vous pouvez gérer vos systèmes d'extrémité grâce à Sophos Central et activer Intercept X pour un déploiement automatique.

Équipe commerciale France :
Tél. : 01 34 34 80 00
Email : info@sophos.fr

Essai gratuit

Inscrivez-vous pour participer à une évaluation gratuite de 30 jours sur sophos.fr/intercept-x

2017-09-10-DS-FR (MP)

SOPHOS