SOPHOS

Intercept X

La meilleure protection Endpoint sur le marché

Sophos Intercept X bloque la plus grande gamme d'attaques avec une combinaison unique de technologies de détection des malwares par Deep Learning, de prévention des exploits, de protection anti-ransomware, et bien plus.

Avantages principaux

- Moteur classé n° 1 pour la détection des malwares, assurée par Deep Learning
- Prévention des exploits qui bloque les techniques utilisées par les attaquants pour contrôler les logiciels vulnérables
- Technologie « Active adversary » pour empêcher la persistance sur une machine
- Analyse détaillée des attaques pour identifier l'activité du malware et son point d'entrée
- Technologie de prévention spécifique aux ransomwares
- Fonctionnalité EDR (Endpoint Detection and Response) qui permet aux administrateurs IT et analystes de sécurité de maintenir l'hygiène des opérations de sécurité informatique et d'optimiser la traque des menaces

Sophos Intercept X déploie une approche de défense en profondeur globale de la protection Endpoint plutôt que de s'appuyer uniquement sur une seule technique de sécurité. C'est ce que nous appelons « la puissance du plus », c'est-à-dire une combinaison de techniques de pointe fondamentales et modernes.

Les techniques modernes incluent la détection des malwares par Deep Learning, la prévention des exploits et des fonctions spécialement conçues pour bloquer les ransomwares. Les techniques fondamentales incluent la détection des malwares basée sur les signatures, l'analyse comportementale, la détection du trafic malveillant, le contrôle des applications, le filtrage Web, la prévention des pertes de données, et bien plus encore.

Détection des malwares par Deep Learning

L'intelligence artificielle intégrée dans Intercept X met en œuvre des techniques de Deep Learning à base de réseaux neuronaux, une forme avancée de Machine Learning, et détecte les malwares connus et inconnus sans avoir recours aux signatures.

Grâce à la puissance du Deep Learning, Intercept X est doté du meilleur moteur de détection des malwares sur le marché, comme l'ont attesté des organismes de contrôle indépendants. Cela permet à Intercept X de détecter les malwares qui ont réussi à contourner les défenses d'autres outils de sécurité Endpoint.

Stopper l'exploit pour stopper l'attaque

De plus en plus de vulnérabilités sont découvertes dans des logiciels, et les éditeurs doivent constamment les corriger. Il est en revanche rare de découvrir de nouvelles techniques d'exploit. En général, ce sont toujours les mêmes techniques qui sont réutilisées par les attaquants. La prévention des exploits stoppe les attaquants en bloquant les outils d'exploit et les techniques utilisés pour diffuser les malwares, voler les identifiants et échapper à la détection. Sophos repousse ainsi les manœuvres d'évitement des pirates et des attaques Zero-day sur votre réseau.

Protection anti-ransomware éprouvée

Intercept X utilise l'analyse comportementale pour bloquer les ransomwares inédits et les attaques sur le secteur de boot, devenant ainsi la technologie anti-ransomware la plus avancée du marché. 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 des ordinateurs distants et des processus locaux qui tentent de modifier vos documents ou d'autres fichiers.

Endpoint Detection and Response (EDR)

Sophos Intercept X Advanced est la première solution EDR conçue pour les administrateurs IT et les analystes de sécurité pour les aider à résoudre les opérations informatiques et traquer les menaces. Il vous permet de poser n'importe quelle question sur un événement passé ou en cours survenant sur vos postes. Traquez les menaces pour détecter les adversaires actifs, ou exploitez les opérations informatiques pour maintenir l'hygiène de la sécurité informatique Lorsqu'un problème est détecté, répondez à distance avec précision.

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.

Managed Threat Response (MTR)

Sophos MTR est une offre de services de recherche, de détection et de remédiation des menaces, entièrement gérée par une équipe d'experts 24 h/24 et 7 j/7. Exploitant la fonctionnalité EDR intégrée dans Intercept X Advanced with EDR, les analystes de Sophos répondent aux menaces, recherchent les indicateurs de compromission et fournissent une analyse des événements qui détaille ce qui s'est produit, où, quand, comment et pourquoi.

Spécifications techniques

Sophos Intercept X prend en charge Windows 7 et supérieur, 32 et 64 bits. Il peut également fonctionner en complément de tout autre produit antivirus ou Endpoint tiers, en y apportant la détection des malwares par Deep Learning, des capacités anti-exploit, anti-ransomware, des rapports détaillés des attaques et Sophos Clean.

	Fonctions	
PRÉVENTION DES EXPLOITS	Application de la Prévention de l'exécution des données	✓
	Distribution aléatoire de l'espace d'adressage (ASLR)	✓
	Bottom-up ASLR	✓
	Null Page (déréférencement du pointeur Null)	✓
	Allocation de heap spray	✓
	Dynamic Heap Spray	✓
	Stack Pivot	✓
	Stack Exec (MemProt)	✓
	Prévention Stack-Based ROP (Caller)	✓
	Prévention des Branch-based ROP (assisté par matériel)	✓
	Structured Exception Handler Overwrite Protection (SEHOP)	✓
	Filtrage des accès à la table d'import (IAF)	✓
	Load Library	✓
	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 de privilèges	✓
PRÉVENTION ACTIVE ADVERSARY	Protection contre le vol des codes d'accès	✓
	Prévention du Code Cave	✓
	Détection MITB (Safe Browsing)	✓
	Détection du trafic malveillant	✓
	Détection des Meterpreter Shell	✓

	Fonctions	
ANTI-RANSOMWARE	Protection des fichiers contre les ransomwares (CryptoGuard)	✓
	Restauration automatique des fichiers (CryptoGuard)	✓
	Protection de l'enregistrement de démarrage et contre la réinitialisation du disque (WipeGuard)	✓
VERROUILLAGE DES APPLICATIONS	Navigateurs Web (y compris HTA)	✓
	Plugins navigateur Web	✓
	Java	✓
	Applications Média	✓
	Applications Office	✓
DEEP LEARNING	Détection des malwares par Deep Learning	✓
	Blocage des applications potentiellement indésirables (PUA) par Deep Learning	✓
	Suppression des faux positifs	✓
	Live Protection	✓
RÉPONSE INVESTIGATION SUPPRESSION	Analyse détaillée des attaques	✓
	Sophos Clean	✓
	Synchronized Security Heartbeat	✓
DÉPLOIEMENT	Peut fonctionner comme un agent autonome	✓
	Peut fonctionner en plus de l'antivirus existant	✓
	Peut fonctionner comme composant de l'agent Sophos Endpoint actuel	✓
	Windows 7	✓
	Windows 8	✓
	Windows 8.1	✓
	Windows 10	✓
	macOS*	✓

* Fonctions prises en charge : CryptoGuard, détection du trafic malveillant (MTD), Synchronized Security Heartbeat, analyse détaillée des attaques (Root Cause Analysis).

Essayez-le gratuitement

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

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

2020-05-11 DSFR (PS)

SOPHOS