SOPHOS

Intercept X Advanced for Server with EDR

Protection inégalée des serveurs

Protégez vos serveurs Cloud, locaux et virtuels contre les malwares, ransomwares et les attaques sans fichiers. L'EDR optimise la traque des menaces et les opérations IT pour vous offrir une visibilité incomparable sur l'ensemble de votre parc informatique.

Avantages principaux

- Sécurisez vos serveurs sur site et vos ressources dans le Cloud
- Protection anti-malware de pointe augmentée par Deep Learning
- Protection « Active Adversary », anti-exploit et anti-ransomware
- 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
- Identification et sécurisation de l'intégralité de votre environnement Cloud, tel que les compartiments S3 et base de données
- Protection des configurations de serveur contre les modifications non autorisées

Bloquez les dernières menaces

Sophos Intercept X for Server déploie une approche de défense en profondeur globale de la protection des serveurs plutôt que de s'appuyer uniquement sur une seule technique de sécurité.

Les techniques modernes incluent l'intelligence artificielle du Deep Learning sans signature, qui excelle à bloquer les malwares inédits. Les capacités anti-ransomware détectent et bloquent les processus de chiffrement malveillants et restaurent les fichiers affectés vers leur état d'origine sain, minimisant les risques d'interruption des activités. Les techniques anti-exploit neutralisent les attaques sans fichiers et les exploits, tels que les scripts PowerShell dissimulés couramment utilisés par les attaquants. 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 protection contre la perte de données, et bien plus encore.

Obtenez une visibilité inégalée

Intercept X Advanced for Server est la première solution EDR conçue pour les administrateurs IT et les analystes de sécurité. Elle les aide à résoudre les opérations informatiques et à traquer les menaces. Par exemple trouver les serveurs dont le protocole RDP (Remote Desktop Protocol) est activé inutilement, combler cette faille de sécurité, puis traquer les processus suspects qui tentent de se connecter sur un port non standard et les bloquer.

Identifiez et sécurisez l'ensemble de votre inventaire multi-Cloud. Vous pouvez détecter vos ressources dans le Cloud ainsi que les services Cloud critiques, dont les compartiments S3, les bases de données et les fonctions sans serveur, identifier les activités suspectes ou les déploiements non sécurisés, et combler les failles de sécurité.

Prenez le contrôle de vos serveurs

Créez rapidement des politiques de sécurité pour protéger contre les menaces et contrôler les applications, les périphériques et le Web, puis appliquez-les à tous vos déploiements Cloud, locaux et virtuels. Les politiques de sécurité peuvent être configurées par serveur. Le verrouillage des serveurs empêche, en un seul clic, les modifications non autorisées pour que seules les applications approuvées puissent s'exécuter – sans temps d'arrêt du serveur. Surveillez les fichiers et dossiers critiques, en recevant une notification en cas de tentative d'altération.

Simplifiez la gestion et le déploiement

Sophos Central facilite la gestion de vos serveurs. Vous pouvez accéder aux politiques de sécurité, aux alertes et aux rapports depuis un seul écran. Sophos Central propose aussi des politiques par défaut et recommande des configurations pour que vous disposiez de la meilleure protection dès le premier jour. Et la politique de licence et l'agent déployé sont les mêmes pour les déploiements physiques, virtuels, Cloud et mixtes.

Sécurisez l'ensemble de votre parc IT

Intercept X for Server protège vos serveurs où qu'ils se trouvent et permet de les gérer facilement depuis la même console. Sécurisez les serveurs physiquement sur site, les instances Amazon EC2, les machines virtuelles Microsoft Azure et Google Cloud, ainsi que les déploiements virtuels et les scénarios mixtes.

Managed Threat Response (MTR)

Sophos MTR est une offre de services de recherche, de détection et de remédiation des menaces, entièrement managée par une équipe d'experts 24 h/24 et 7 j/7. Exploitant la fonctionnalité EDR intégrée dans Intercept X Advanced for Server 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.

FONCTIONNALITÉS	
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 (falsification de la pile)	✓
Stack Exec (MemProt)	✓
Prévention Stack-Based ROP (Caller)	✓
Prévention 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	✓
Hollow Process	✓
DLL Hijacking	✓
Squiblydoo AppLocker Bypass	✓
Protection APC (Double Pulsar/AtomBombing)	✓
Processus d'élévation de privilèges	✓
Protection shellcode dynamique	✓
EFS Guard	✓
CTF Guard	✓
ApiSetGuard	✓

FONCTIONNALITÉS	
PRÉVENTION « ACTIVE ADVERSARY »	
Protection contre le vol des codes d'accès	✓
Prévention du Code Cave	✓
Détection MITB (Safe Browsing)	✓
Détection du trafic malveillant (MTD)	✓
Détection des Meterpreter Shell	✓
ANTI-RANSOMWARE	
Protection des fichiers contre les ransomwares (CryptoGuard)	✓
Restauration automatique des fichiers (CryptoGuard)	✓
Protection du secteur de boot et contre la réinitialisation du disque (WipeGuard)	✓
VERROUILLAGE DES APPLICATIONS	
Navigateurs Web (y compris HTA)	✓
Plugins navigateur Web	✓
Java	✓
Applications Média	✓
Applications Office	✓
PROTECTION PAR DEEP LEARNING	
Détection des malwares par Deep Learning	✓
Blocage des applications potentiellement indésirables (PUA) par Deep Learning	✓
RÉPONSE/INVESTIGATION/SUPPRESSION	
Suppression des faux positifs	✓
Dossiers Menace (analyse RCA)	✓
Sophos Clean	✓
Synchronized Security Heartbeat	✓

Essayez-le gratuitement dès aujourd'hui

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

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

20-07-21 DS-FR (DD)

SOPHOS