SOPHOS
Cybersecurity made simple.

CLOUD READY

Intercept X for Server

Que ce soit dans le Cloud ou en local, vous avez besoin de protéger les applications et les données critiques au cœur de votre entreprise. Intercept X for Server offre une approche de défense en profondeur, avec la détection des malwares par Deep Learning, la prévention des exploits, une technologie anti-ransomware, la mise sur liste blanche des applications, la protection contre le piratage et l'analyse détaillée des attaques.

Principaux avantages

- Découvre et protège les ressources dans Microsoft Azure et Amazon Web Services
- Protège les serveurs des ransomwares, y compris des attaques distantes depuis un système malveillant
- Mise sur liste blanche grâce au verrouillage des serveurs
- Bloque les techniques avancées de piratage et d'exploits
- Analyse détaillée des attaques pour connaître l'origine d'une attaque et le chemin d'infection
- Sécurité synchronisée qui partage les données sur les menaces, le statut de santé et la sécurité entre une multitude de produits Sophos
- Gestion simplifiée depuis Sophos Central
- Protection des systèmes Windows et Linux contre les menaces

Une protection puissante élaborée pour les serveurs

Intercept X for Server exploite un grand nombre de technologies pour stopper les attaques Zero-day, les exploits et les piratages. Ces protections empêchent les attaques d'atteindre en premier lieu les serveurs, détectent les attaques avant qu'elles ne s'exécutent ou, si ces dernières parviennent à contourner la protection, elles les stoppent et nettoient le serveur en profondeur. Son modèle d'intelligence artificielle constamment mis à jour est formé pour rechercher sur les serveurs les attributs suspects des codes malveillants. En outre, les fonctions spécifiques aux serveurs, comme le verrouillage des serveurs et la découverte des charges de travail Cloud, garantissent la sécurité des configurations de serveur.

Intercept X for Server découvre et protège les ressources dans le Cloud, dont Microsoft Azure et Amazon Web Services. En connectant Sophos Central avec AWS et Azure, Intercept X for Server affiche de manière visuelle dans Sophos Central les informations pertinentes sur les serveurs protégés.

Stoppez les ransomwares spécifiques aux serveurs

CryptoGuard protège contre les ransomwares à l'échelle des fichiers systèmes pour détecter et intercepter le chiffrement non sollicité des fichiers, que ce soit sur le serveur ou depuis un système distant connecté au serveur. De manière similaire, WipeGuard protège l'enregistrement d'amorçage maître contre le chiffrement malveillant.

Sophos Intercept X for Server verrouille votre serveur d'un simple clic, mettant sur liste blanche vos applications afin de sécuriser votre serveur dans état sain et empêchant les applications non autorisées de s'exécuter. Sophos analyse automatiquement le système et établit un inventaire (liste blanche) des applications saines connues, sans besoin de créer de règles manuelles. Sophos créé un lien incassable entre les applications et les fichiers associés, tels que les fichiers de données, les fichiers DLL et les scripts.

Repoussez les attaques : Empêchez les pirates d'accéder au serveur

Les vulnérabilités apparaissent à un rythme alarmant, et corriger les serveurs sans perturber les utilisateurs peut se révéler difficile. Les attaques d'exploits peuvent être désastreuses et ne sont souvent pas détectées par les technologies traditionnelles de protection des serveurs. Intercept X for Server est conçu pour empêcher même les pirates les plus tenaces d'utiliser des techniques d'exploit pour collecter des identifiants de connexion. Que leur objectif soit de rester incognito et persistant ou de migrer latéralement, Intercept X est conçu pour les arrêter.

Analyse détaillée des attaques (RCA)

Intercept X for Server inclut également une technologie de détection et de réponse qui offre une visibilité complète pour que les administrateurs puissent déterminer le point d'entrée de l'attaque, son cheminement, ce qu'elle a touché, et les mesures à prendre en conséquence. Intercept X for Server fournit ce service sans nécessiter d'agent ou de console d'administration supplémentaire.

Sécurité synchronisée

La sécurité synchronisée est un système de sécurité de pointe qui permet à vos défenses d'être aussi coordonnées que les attaques auxquelles elles font face. Elle associe une plateforme de sécurité intuitive avec des produits multi-primés qui fonctionnent ensemble pour bloquer les menaces avancées et offrir une protection inégalée.

Principales fonctions d'Intercept X for Server

PLATE-FORMES		Windows Server	✓
		Linux[1]	✓
		Cloud public (Microsoft Azure et Amazon AWS)	✓
PRÉVENTION	RÉDUCTION DE LA SURFACE D'ATTAQUE	Mise sur liste blanche des applications (verrouillage des serveurs)	✓
		Sécurité du Web	✓
		Windows Firewall Control	✓
		Réputation des téléchargements	✓
		Contrôle du Web (blocage des URL)	✓
		Contrôle des périphériques (par ex. clé USB)	✓
		Contrôle des applications	✓
	AVANT EXECUTION SUR LE SYSTEME	Détection des malwares par Deep Learning	✓
		Prévention contre les exploits	✓
		Analyse antimalware des fichiers	✓
		Live Protection	✓
		Analyse comportementale avant l'exécution (HIPS)	✓
		Contrôle non embarqué pour les MV (ESXi et Hyper-V)[2]	✓
		Détection des applications potentiellement indésirables (PUA)	✓
		Prévention des pertes de données	✓
DÉTECTION	BLOQUE LES MENACES EN COURS D'EXÉCUTION	Prévention du piratage	✓
		Protection des fichiers contre les ransomwares (CryptoGuard) inclut la détection des attaques sur le serveur depuis un terminal connecté à distance	✓
		Protection de l'enregistrement de démarrage et contre la réinitialisation du disque (WipeGuard)	✓
		Détection du trafic malveillant	✓
RÉPONSE	INVESTIGATION ET SUPPRESSION	Suppression automatique des malwares avec Sophos Clean	✓
		Analyse détaillée des attaques (RCA)	✓
GESTION	CONTRÔLE	Gestion des politiques spécifiques aux serveurs	✓
		Cache de mise à jour et Relais de messages	✓
		Exclusions automatiques des contrôles	✓
		Contrôle synchronisé des applications[4]	✓
	VISIBILITÉ	Découverte et protection des ressources Azure	✓
		Découverte et protection des ressources AWS	✓
		Carte AWS, visualisation multi-régions	✓
		Synchronized Security avec Security Heartbeat™ (Protection contre les menaces, identification positive de la source et isolement automatisé améliorés)[4]	✓
		Services Bureau à distance de Windows (visibilité utilisateur)	✓
	SOPHOS CENTRAL	Gestion basée dans le Cloud, éliminant le besoin d'installer et de maintenir un serveur séparé en local, et gestion de la sécurité des serveurs depuis une seule console en parallèle de la sécurité des systèmes Endpoint, des mobiles, des messageries et des réseaux sans fil.	✓
		Authentification multifacteur	✓
		Administration déléguée	✓

Gestion simple avec Sophos Central

Gérer votre sécurité depuis Sophos Central signifie que vous n'avez plus besoin de déployer un serveur pour sécuriser vos systèmes Endpoint. Hébergé par Sophos, Sophos Central offre un accès instantané sans nécessiter l'installation d'une console serveur dédiée. Sophos Central fournit des politiques de sécurité prêtes à l'emploi pour les serveurs et permet la gestion en parallèle d'autres produits Sophos, dont Sophos Intercept X, Mobile, Wireless, Email et Web. Le tout depuis un seul écran.

1 Toutes les fonctions sont disponibles sous Windows, certaines fonctions sont disponibles sous Linux.
2 Voir le Guide de gestion des licences pour Sophos for Virtual Environments, agent de déploiement ultrafin.
3 Pour les serveurs Windows gérés par Sophos Enterprise Console, CryptoGuard est disponible avec la licence complémentaire Endpoint Exploit Prevention (EXP).
4 Lorsqu'il est utilisé en conjonction avec Sophos XG Firewall.

Azure

aws partner network
Advanced Technology Partner
Security Competency
Public Sector Partner
Marketplace Seller

Essayez-le gratuitement dès aujourd'hui

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

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

28/06/2018 DS-FR (MP)

SOPHOS