Intercept X for Server, XDR et MTR - Vue d'ensemble

SOPHOS

Administrés dans Sophos Central

	Fonctionnalités	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
GESTION	Plusieurs politiques		✓	✓	✓	✓
	Mises à jour contrôlées		✓	✓	✓	✓
RÉDUCTION DE LA SURFACE D'ATTAQUE	Contrôle des applications		✓	✓	✓	✓
	Contrôle des périphériques		✓	✓	✓	✓
	Contrôle du Web/Blocage des URL par catégories		✓	✓	✓	✓
	Liste d'autorisation des applications (verrouillage du serveur)		✓	✓	✓	✓
	Réputation des téléchargements	✓	✓	✓	✓	✓
	Sécurité du Web	✓	✓	✓	✓	✓
AVANT EXÉCUTION SUR LE SYSTÈME	Détection des malwares par Deep Learning	✓	✓	✓	✓	✓
	Analyse antimalware des fichiers	✓	✓	✓	✓	✓
	Live Protection	✓	✓	✓	✓	✓
	Analyse comportementale avant l'exécution (HIPS)	✓	✓	✓	✓	✓
	Blocage des applications potentiellement indésirables (PUA)	✓	✓	✓	✓	✓
	Système de prévention des intrusions (IPS)	✓	✓	✓	✓	✓
BLOQUE LES MENACES EN COURS D'EXÉCUTION	Protection contre la perte de données (DLP)	✓	✓	✓	✓	✓
	Analyse comportementale runtime (HIPS)	✓	✓	✓	✓	✓
	Antimalware Scan Interface (AMSI)	✓	✓	✓	✓	✓
	Détection du trafic malveillant (MTD)	✓	✓	✓	✓	✓
	Prévention anti-exploit (détails p.5)	✓	✓	✓	✓	✓
	Prévention Active Adversary (détails p.5)	✓	✓	✓	✓	✓
	Protection des fichiers contre les ransomwares (CryptoGuard)	✓	✓	✓	✓	✓
	Protection du secteur de boot et contre la réinitialisation du disque (WipeGuard)	✓	✓	✓	✓	✓
	Détection MITB (Safe Browsing)	✓	✓	✓	✓	✓
	Amélioration du verrouillage des applications	✓	✓	✓	✓	✓

Suite des fonctionnalités à la page suivante

Intercept X for Server, XDR et MTR - Vue d'ensemble

SOPHOS

Administrés dans Sophos Central

	Fonctionnalités	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
DÉTECTION	Live Discover (Requêtes SQL pour la traque des menaces et l'hygiène des opérations de sécurité IT sur l'ensemble du parc informatique)			✓	✓	✓
	Bibliothèque de requêtes SQL (pré-écrites, entièrement personnalisables)			✓	✓	✓
	Stockage des données sur disque avec accès rapide (jusqu'à 90 jours)			✓	✓	✓
	Sources de données inter-produits par ex. Firewall, Email			✓	✓	✓
	Requêtes inter-produits			✓	✓	✓
	Sophos Data Lake (Stockage de données dans le Cloud)			30 jours	30 jours	30 jours
	Requêtes programmées			✓	✓	✓
INVESTIGATION	Dossiers Menace (analyse RCA)		✓	✓	✓	✓
	Analyses des malwares par Deep Learning			✓	✓	✓
	Intelligence sur les menaces des SophosLabs à la demande			✓	✓	✓
	Exportation de données d'investigation			✓	✓	✓
REMÉDIATION	Suppression automatique des malwares	✓	✓	✓	✓	✓
	Synchronized Security Heartbeat	✓	✓	✓	✓	✓
	Sophos Clean	✓	✓	✓	✓	✓
	Live Response (Accès distant au terminal pour des analyses et une réponse plus poussées)			✓	✓	✓
	Isolement du serveur à la demande			✓	✓	✓
	« Nettoyer et bloquer » en un seul clic			✓	✓	✓
VISIBILITÉ	Protection des charges de travail Cloud (Amazon Web Services, Microsoft Azure, Google Cloud Platform)	✓	✓	✓	✓	✓
	Contrôle synchronisé des applications (visibilité des applications)	✓	✓	✓	✓	✓
	Gestion de la posture de sécurité Cloud (surveillance et protection des hébergements Cloud, fonctions sans serveur, compartiments S3, etc.)		✓	✓	✓	✓

Intercept X for Server, XDR et MTR - Vue d'ensemble

SOPHOS

Administrés dans Sophos Central

	Fonctionnalités	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
CONTRÔLE	Cache de mise à jour et Relais de messages	✓	✓	✓	✓	✓
	Exclusions automatiques des contrôles	✓	✓	✓	✓	✓
	Surveillance de l'intégrité des fichiers		✓	✓	✓	✓
SERVICE MANAGÉ	Traque des menaces à partir d'indices 24/7				✓	✓
	Diagnostics de sécurité				✓	✓
	Conservation des données				✓	✓
	Rapport d'activité				✓	✓
	Détections des adversaires				✓	✓
	Neutralisation et remédiation des menaces				✓	✓
	Traque des menaces sans indices de départ 24/7					✓
	Responsable de la réponse aux menaces dédié					✓
	Assistance téléphonique directe					✓
	Gestion proactive de la posture de sécurité					✓

Comparaison des fonctionnalités par système d'exploitation

SOPHOS

	FONCTIONNALITÉS	WINDOWS	LINUX*
GESTION	Plusieurs politiques	✓	✓
	Mises à jour contrôlées	✓	✓
RÉDUCTION DE LA SURFACE D'ATTAQUE	Sécurité du Web	✓	
	Réputation des téléchargements	✓	
	Contrôle du Web / Blocage des URL par catégories	✓	
	Contrôle des périphériques	✓	
	Contrôle des applications	✓	
	Liste d'autorisation des applications (verrouillage du serveur)	✓	
AVANT EXÉCUTION SUR LE SYSTÈME	Détection des malwares par Deep Learning	✓	✓
	Analyse antimalware des fichiers	✓	✓
	Live Protection	✓	✓
	Analyse comportementale avant l'exécution (HIPS)	✓	
	Blocage des applications potentiellement indésirables (PUA)	✓	
	Système de prévention des intrusions (IPS)	✓	
BLOQUE LES MENACES EN COURS D'EXÉCUTION	Prévention des pertes de données (DLP)	✓	
	Analyse comportementale runtime (HIPS)	✓	
	Antimalware Scan Interface (AMSI)	✓	
	Détection du trafic malveillant (MTD)	✓	Voir note
	Prévention anti-exploit (détails p.5)	✓	
	Prévention Active Adversary (détails p.5)	✓	
	Protection des fichiers contre les ransomwares (CryptoGuard)	✓	
	Protection du secteur de boot et contre la réinitialisation du disque (WipeGuard)	✓	
	Détection MITB (Safe Browsing)	✓	
	Amélioration du verrouillage des applications	✓	

Suite des fonctionnalités à la page suivante

Comparaison des fonctionnalités par système d'exploitation

SOPHOS

	FONCTIONNALITÉS	WINDOWS	LINUX*
DÉTECTION	Live Discover (Requêtes SQL pour la traque des menaces et l'hygiène des opérations de sécurité IT sur l'ensemble du parc informatique)	✓	✓
	Bibliothèque de requêtes SQL (pré-écrites, entièrement personnalisables)	✓	✓
	Stockage des données sur disque avec accès rapide (jusqu'à 90 jours)	✓	✓
	Sources de données inter-produits par ex. Firewall, Email	✓	✓
	Requêtes inter-produits	✓	✓
	Sophos Data Lake (Stockage de données dans le Cloud)	✓	✓
	Requêtes programmées	✓	✓
INVESTIGATION	Dossiers Menace (analyse RCA)	✓	
	Analyses des malwares par Deep Learning	✓	
	Intelligence sur les menaces des SophosLabs à la demande	✓	
	Exportation de données d'investigation	✓	
REMÉDIATION	Suppression automatique des malwares	✓	
	Synchronized Security Heartbeat	✓	Voir note
	Sophos Clean	✓	
	Live Response (Accès distant au terminal pour des analyses et une réponse plus poussées)	✓	✓
	Isolement du serveur à la demande	✓	
	« Nettoyer et bloquer » en un seul clic	✓	
VISIBILITÉ	Protection des workloads Cloud (Amazon Web Services, Microsoft Azure, Google Cloud Platform)	✓	✓
	Contrôle synchronisé des applications (visibilité des applications)	✓	
	Gestion de la posture de sécurité Cloud (surveillance et protection des hébergements Cloud, fonctions sans serveur, compartiments S3, etc.)	✓	✓
CONTRÔLE	Cache de mise à jour et Relais de messages	✓	
	Exclusions automatiques des contrôles	✓	
	Surveillance de l'intégrité des fichiers	✓	

Comparaison des fonctionnalités par système d'exploitation

SOPHOS

	FONCTIONNALITÉS	WINDOWS	LINUX*
SERVICE MANAGÉ	Traque des menaces à partir d'indices 24/7	✓	✓
	Diagnostics de sécurité	✓	✓
	Conservation des données	✓	✓
	Rapport d'activité	✓	✓
	Détections des adversaires	✓	✓
	Neutralisation et remédiation des menaces	✓	✓
	Traque des menaces sans indices de départ 24/7	✓	✓
	Responsable de la réponse aux menaces dédié	✓	✓
	Assistance téléphonique directe	✓	✓
	Amélioration proactive de la posture de sécurité	✓	✓

*Linux inclut deux options de déploiement. 1) Le déploiement de Sophos Protection pour Linux donne accès aux fonctionnalités indiquées dans le tableau. 2) Le déploiement de Sophos Anti-Virus pour Linux comprend : Anti-malware, Live Protection, Détection du trafic malveillant et Sécurité Synchronisée. Veuillez noter que les deux options de déploiement ne peuvent pas être utilisées ensemble.

Les fonctionnalités de Sophos Intercept X

Détail des fonctionnalités incluses dans Intercept X

	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 (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	✓
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	✓

	Fonctionnalités	
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	✓
	Suppression des faux positifs	✓
RÉPONSE INVESTIGATION SUPPRESSION	Dossiers Menace (analyse RCA)	✓
	Sophos Clean	✓
	Synchronized Security Heartbeat	✓

Managed Threat Response (MTR)

Sophos MTR (Managed Threat Response) est une offre de services de recherche, de détection et de remédiation des menaces, entièrement gérés par une équipe d'experts, 24 h/24 et 7 j/7. Les clients MTR reçoivent aussi Intercept X Advanced for Server with XDR.

Sophos MTR : Standard

Traque des menaces à partir d'indices 24/7

Les activités et artefacts malveillants confirmés (signaux forts) sont automatiquement bloqués ou supprimés. Les analystes peuvent ainsi consacrer tous leurs efforts à traquer et à remonter la piste des menaces. Ce type de recherche consiste à agréger et à analyser les facteurs de causalité et les événements connexes (signaux faibles) pour découvrir de nouveaux indicateurs d'attaque (IoA) et indicateurs de compromission (IoC) qui n'étaient pas détectés auparavant.

Diagnostic de sécurité

Maintenez vos produits Sophos Central, en commençant par Intercept X Advanced for Server with XDR, à un niveau de performances optimales par un examen proactif de vos conditions d'exploitation et par des recommandations pour améliorer vos configurations.

Rapport d'activité

Les résumés des événements permettent d'établir les priorités et de vous informer, de sorte que votre équipe sait quelles menaces ont été détectées et quelles mesures ont été prises entre chaque rapport.

Détections des adversaires

Une grande partie des attaques réussies ont utilisé un processus semblant légitime pour tromper les outils de surveillance. En utilisant des techniques d'investigation exclusives, notre équipe détermine la différence entre un comportement légitime et les tactiques, techniques et procédures utilisées par les attaquants.

Sophos MTR : Advanced *Toutes les fonctionnalités du niveau Standard + les éléments suivants :*

Traque des menaces sans indices de départ 24/7

En nous basant sur la science des données, l'intelligence sur les menaces et l'intuition d'experts chevronnés, nous prenons en compte le profil de votre société, vos ressources de grande valeur et vos utilisateurs les plus à risque pour anticiper le comportement des pirates et identifier de nouveaux indicateurs d'attaque (IOA).

Données télémétriques améliorées

L'investigation des menaces est complétée par des données télémétriques issues des autres produits Sophos Central, qui, en allant au-delà du système d'extrémité, fournissent une image complète des activités malveillantes.

Amélioration proactive de la posture de sécurité

Des recommandations vous aident à améliorer de manière proactive votre posture de sécurité et à renforcer vos défenses en corrigeant les lacunes de la configuration et de l'architecture, augmentant ainsi vos capacités de sécurité globales.

Interlocuteur dédié en cas d'incident

Lorsqu'un incident est confirmé, vous pouvez contacter un interlocuteur dédié dont la mission est de collaborer directement avec votre personnel sur site (équipe interne ou partenaire externe) jusqu'à ce que la menace active soit neutralisée.

Assistance téléphonique directe

Votre équipe peut appeler directement notre centre d'opérations et de sécurité (SOC). Notre équipe MTR opérationnelle est disponible 24 h/24 et s'appuie sur nos équipes du support technique réparties sur 26 sites dans le monde entier.

Découverte des ressources

De l'information sur les ressources, comprenant les versions du système d'exploitation, les applications et les vulnérabilités, à l'identification des ressources gérées et non gérées, nous fournissons des informations précieuses pour évaluer l'impact d'un incident, traquer les menaces et fournir des conseils pour améliorer de manière proactive la posture globale de sécurité.

SOPHOS