Guide des licences Sophos Workload Protection

SOPHOS
Cybersecurity delivered.

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

Administrés dans Sophos Central

Fonctionnalités	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	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)	✓	✓	✓	✓	✓	✓

Fonctionnalités	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
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	✓	✓	✓	✓	✓	✓
Détection						
Live Discover (Requêtes SQL pour la chasse aux 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			✓	✓	✓	✓
Liste des détections classées par ordre de priorité			✓	✓	✓	✓
Sophos Data Lake (Stockage de données dans le Cloud)			30 jours	30 jours	30 jours	30 jours
Requêtes programmées			✓	✓	✓	✓
Visibilité et détections runtime du conteneur			✓	✓	✓	✓
Investigation						
Dossiers Menace (analyse RCA)		✓	✓	✓	✓	✓
Analyses des malwares par Deep Learning			✓	✓	✓	✓
Renseignements sur les menaces collectés par les SophosLabs, à la demande			✓	✓	✓	✓
Exportation de données d'investigation			✓	✓	✓	✓
Investigations guidées par l'IA			✓	✓	✓	✓

Fonctionnalités	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Remédiation						
Suppression automatique des malwares	✓	✓	✓	✓	✓	✓
Security Heartbeat synchronisé	✓	✓	✓	✓	✓	✓
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 et détections runtime du conteneur			✓	✓	✓	✓
Contrôle						
Contrôle synchronisé des applications (visibilité des applications)	✓	✓	✓	✓	✓	✓
Cache de mise à jour et Relais de messages	✓	✓	✓	✓	✓	✓
Exclusions automatiques des contrôles	✓	✓	✓	✓	✓	✓
Surveillance de l'intégrité des fichiers			✓	✓	✓	✓
Environnements Cloud						
Surveillance de l'environnement Cloud : AWS, Azure, GCP, Kubernetes, IaC et registres Docker Hub		Un par fournisseur	Un par fournisseur	Illimité	Un par fournisseur	Un par fournisseur
Surveillance de la sécurité (Règles des bonnes pratiques CSPM)		Analyses quotidiennes	Analyses quotidiennes	Analyses planifiées, quotidiennes et à la demande	Analyses quotidiennes	Analyses quotidiennes
Inventaire des ressources		✓	✓	✓	✓	✓
Fonctions de recherche avancée		✓	✓	✓	✓	✓
Détection des anomalies optimisée par l'IA		✓	✓	✓	✓	✓
Alertes de trafic malveillant par SophosLabs Intelix		✓	✓	✓	✓	✓
Alertes par email		✓	✓	✓	✓	✓
Intégrations de services AWS natifs (Amazon GuardDuty, AWS Security Hub, Amazon Inspector, etc.)		✓	✓	✓	✓	✓
Intégrations de services Azure natifs (Azure Sentinel et Advisor)		✓	✓	✓	✓	✓
Cloud Workload Protection : Découverte de l'agent Sophos Intercept X Server		✓	✓	✓	✓	✓
Cloud Workload Protection : Suppression automatique de l'agent Sophos Intercept X Server		✓	✓	✓	✓	✓

Fonctionnalités	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Politiques et rapports de conformité		Critères CIS	Critères CIS	Critères CIS, ISO 27001, EBU R 143, FEDRAMP FIEC, GDPR, HIPAA, PCI DSS, SOC2, Bonnes pratiques de Sophos	Critères CIS	Critères CIS
Politiques personnalisées				✓		
Visualisation du réseau		✓	✓	✓	✓	✓
Visualisation de l'IAM		✓	✓	✓	✓	✓
Surveillance des dépenses		✓	✓	✓	✓	✓
Intégrations de la gestion des alertes (Jira, ServiceNow, Slack, Teams, PagerDuty, Amazon SNS)		✓	✓	✓	✓	✓
Intégrations SIEM (Splunk, Azure Sentinel)		✓	✓	✓	✓	✓
API Rest		✓	✓	✓	✓	✓
Analyse des modèles d'infrastructure programmable (IaC)		✓	✓	✓	✓	✓
Contrôle de l'accès à l'environnement		✓	✓	✓	✓	✓
Analyse des images de conteneur (ECR, ACR, Docker Hub, API)		✓	✓	✓	✓	✓
Service managé						
Chasse aux menaces à partir d'indices 24/7					✓	✓
Diagnostics de sécurité					✓	✓
Conservation des données					✓	✓
Rapport d'activité					✓	✓
Détections des adversaires					✓	✓
Neutralisation et remédiation des menaces					✓	✓
Chasse aux menaces sans indices de départ 24/7						✓
Responsable de la réponse aux menaces dédié						✓
Assistance téléphonique directe						✓
Gestion proactive de la posture de sécurité						✓
Protection des fichiers contre les ransomwares (CryptoGuard)						✓

Comparaison des fonctionnalités par système d'exploitation

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		
Protection contre la perte 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	✓	

Fonctionnalités	Windows	Linux*
Détection		
Live Discover (Requêtes SQL pour la chasse aux 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	✓	✓
Liste des détections classées par ordre de priorité	✓	✓
Sophos Data Lake (Stockage de données dans le Cloud)	✓	✓
Requêtes programmées	✓	✓
Visibilité et détections runtime du conteneur		✓
Investigation		
Dossiers Menace (analyse RCA)	✓	
Analyses des malwares par Deep Learning	✓	
Renseignements sur les menaces collectés par les SophosLabs, à la demande	✓	
Exportation de données d'investigation	✓	
Investigations guidées par l'IA	✓	✓
Remédiation		
Suppression automatique des malwares	✓	
Security Heartbeat synchronisé	✓	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	✓	
Contrôle		
Contrôle synchronisé des applications (visibilité des applications)	✓	
Cache de mise à jour et Relais de messages	✓	
Exclusions automatiques des contrôles	✓	

Fonctionnalités	Windows	Linux*
Surveillance de l'intégrité des fichiers	✓	
Service managé		
Chasse aux menaces à partir d'indices 24/7	✓	✓
Diagnostics de sécurité	✓	✓
Conservation des données	✓	✓
Rapport d'activité	✓	✓
Détections des adversaires	✓	✓
Neutralisation et remédiation des menaces	✓	✓
Chasse aux 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.

Aperçu de la protection Sophos

Détails des fonctionnalités de Sophos Workload Protection incluses avec Intercept X et Cloud Native Security

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	✓
Contournement de Squiblydoo AppLocker	✓
Protection APC (Double Pulsar / AtomBombing)	✓
Processus d'élévation de privilèges	✓
Protection shellcode dynamique	✓
EFS Guard	✓

Fonctionnalités	
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	✓
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	✓
Security Heartbeat synchronisé	✓

Managed Threat Response (MTR)

Sophos MTR (Managed Threat Response) est une offre de services de chasse aux menaces, de détection et de réponse, entièrement managés 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

Chasse des menaces à partir d'indices 24 h/24 7j/7
Les activités et artefacts malveillants confirmés (signaux forts) sont automatiquement bloqués ou supprimés. Les analystes peuvent ainsi consacrer tous leurs efforts à chasser 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 de fonctionnement 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 (TTP) utilisées par les attaquants.

Sophos MTR : Advanced

Inclut les fonctionnalités du niveau Standard + les éléments suivants :

Chasse aux menaces sans indices de départ 24/7
En nous basant sur la science des données, la collecte de renseignements 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 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 France
Tél. : 01 34 34 80 00
Email : partners@sophos.fr

© Copyright 2022. Sophos Ltd. Tous droits réservés.
Immatriculée en Angleterre et au Pays de Galles N° 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni.
Sophos est la marque déposée de Sophos Ltd. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

22-07-25 FR (DD)

SOPHOS