Server Workload Protection

Protection de Linux

Intercept X Advanced for Server, Intercept X Advanced for Server with XDR et Intercept X Advanced for Server with MDR

Cloud ou datacenter, hôte et conteneur. Protégez votre infrastructure dès maintenant et au fur et à mesure de son évolution grâce à Sophos Workload Protection, une solution de haut niveau mais à faible impact sur les performances.

Minimisez le temps de détection et de réponse

Obtenez une visibilité complète sur les charges de travail de vos hôtes et de vos conteneurs, en identifiant les logiciels malveillants, les exploits et les comportements anormaux avant qu'ils ne puissent s'implanter. Les capacités XDR (Extended Detection and Response) offrent une vue détaillée sur les hôtes, les conteneurs, les endpoints, le trafic réseau et les services de sécurité natifs du fournisseur de Cloud.

Les fonctions de détection Cloud native identifient les comportements malveillants et les exploits au moment du runtime, notamment l'évasion des conteneurs, l'exploitation du noyau et les tentatives d'élévation des privilèges. Le processus d'investigation des menaces priorise les détections d'incidents à haut risque et consolide les événements connectés pour accroître l'efficacité et gagner du temps.

Améliorez les opérations de sécurité

Neutralisez les menaces grâce aux fonctions de visibilité et de détection des menaces lors du runtime des hôtes et des conteneurs. Ces fonctions sont fournies via notre console de gestion centralisée ou peuvent être intégrées à vos outils de réponse aux menaces existants grâce à nos différentes options de déploiement.

Gestion dans Sophos Central - L'agent Linux léger fournit aux équipes de sécurité les informations essentielles dont elles ont besoin pour analyser et répondre aux comportements à risque, aux exploits et aux malwares depuis une seule console. En surveillant l'hôte Linux, cette option de déploiement permet aux équipes de gérer toutes les solutions Sophos à partir d'une seule et même interface. Elles peuvent ainsi passer en toute transparence de la chasse aux menaces au nettoyage et à la gestion.

Intégration par API - Sophos Linux Sensor est une option de déploiement très flexible qui offre les meilleures performances possibles. Le capteur Linux utilise des API pour intégrer la détection des menaces au runtime, dans les environnements hôtes et les conteneurs, avec vos outils de réponse aux menaces. Il offre un plus grand nombre de détections, la possibilité de créer des ensembles de règles personnalisées et des options de configuration pour ajuster l'utilisation des ressources de l'hôte.

Obtenez des performances stables

La protection d'Intercept X for Server est optimisée pour les workflows DevSecOps, identifiant les attaques sophistiquées au moment où elles se produisent sans nécessiter de module de noyau, d'orchestration, de baseline ou de scans du système. Des limites de ressources optimisées, notamment en termes de CPU, de mémoire et de collecte de données, permettent d'éviter les temps d'arrêt coûteux dus à la surcharge des hôtes et aux problèmes de stabilité. Cela vous permet d'optimiser les performances et la disponibilité des applications.

Avantages principaux

- Protège les charges de travail et des conteneurs Linux Cloud, locaux et virtuels
- Réduit le temps de détection et de réponse aux menaces
- Optimisé pour les charges de travail critiques où les performances sont cruciales
- Exploitez les données Endpoint, réseau, messagerie, Cloud, M365 et mobiles grâce aux capacités XDR (Extended Detection and Response)
- Comprenez et sécurisez votre environnement Cloud élargi grâce à la gestion de la posture de sécurité du Cloud incluse
- Service de sécurité entièrement managé 24/7/365

SOPHOS

Automatisez la vérification de votre sécurité du Cloud

Concevez votre environnement de Cloud pour qu'il réponde aux normes de bonnes pratiques, avec la visibilité et les outils nécessaires pour les maintenir grâce à une gestion intégrée de la posture de sécurité du Cloud couvrant votre environnement de Cloud public plus large :

- Identifiez proactivement les activités non autorisées, les vulnérabilités des images d'hôtes et de conteneurs et les erreurs de configuration sur Amazon AWS, Microsoft Azure et Google Cloud Platform (GCP).
- Découvrez en continu les ressources Cloud grâce à l'inventaire détaillé et la visibilité fournis par la protection Sophos des hôtes et les déploiements de Sophos Firewall.
- Appliquez automatiquement les normes de bonnes pratiques de sécurité pour détecter les failles dans la posture, identifier les gains rapides et les problèmes critiques.
- Détectez les anomalies à haut risque dans le comportement des rôles IAM des utilisateurs, en identifiant rapidement les schémas d'accès inhabituels, les emplacements et les comportements malveillants, afin d'éviter toute violation.

Un partenariat qui renforce votre équipe

Les analystes SOC de haut vol de Sophos Managed Detection and Response (MDR) travaillent en partenariat avec votre équipe, surveillant votre environnement 24 h/24, 7 j/7 et 365 j/an, et chassent de manière proactive les menaces et y remédiant en votre nom, avec l'expertise Linux nécessaire pour gagner en efficacité. Les analystes Sophos répondent aux menaces, recherchent les indicateurs de compromission et fournissent une analyse détaillée des événements, notamment ce qui s'est passé, où, quand, comment et pourquoi.

Spécifications techniques

Pour les dernières informations, veuillez lire la configuration requise pour Linux. Pour plus d'informations sur les fonctionnalités pour Windows, voir la fiche technique Windows.

Fonctionnalités	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MDR Complete
Agent de protection Linux (dont l'analyse des malwares, la prévention anti-exploit, l'analyse des fichiers, etc.)	✔	✔	✔
Capteur Linux (Intégration des détections de menaces lors du runtime de Linux et des conteneurs à vos outils de réponse aux menaces actuels via une API)		✔	✔
Sécurité de l'infrastructure Cloud (Surveillance de la posture de sécurité du Cloud pour prévenir les risques de sécurité et de conformité)	✔	✔	✔
XDR (Extended Detection and Response)		✔	✔
MDR (Managed Detection and Response – service 24/7/365 de chasse et de réponse aux menaces)			✔

Essai gratuit dès aujourd'hui

Évaluation gratuite de 30 jours
sur sophos.fr/server

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

22-10-21 DS-FR (PC)

SOPHOS