SOPHOS
Cybersecurity made simple.

Intercept X Advanced with EDR

Fonctionnalité intelligente « Endpoint Detection and Response » (EDR)
Sophos Intercept X Advanced with EDR intègre la fonctionnalité intelligente EDR au sein de la meilleure protection contre les malwares et les exploits du marché, ainsi que d'autres fonctions inégalées de protection Endpoint.

Avantages principaux

- Fonctionnalité EDR associée à la meilleure protection Endpoint
- Analyses des malwares par Deep Learning
- Intelligence des SophosLabs sur les menaces à la demande
- Détection et hiérarchisation par Machine Learning des événements suspects*
- Investigations guidées pour un EDR accessible mais puissant
- Réponse aux incidents en un seul clic

L'EDR s'appuie sur la meilleure protection possible

Pour empêcher toute violation, le maître mot est la prévention. Intercept X consolide en une seule solution une protection inégalée et la fonction de détection et de réponse des terminaux. La plupart des menaces sont ainsi bloquées avant même de pouvoir occasionner le moindre dégât. Grâce à sa capacité à détecter les menaces potentielles, à les identifier et à y remédier, Intercept X Advanced with EDR offre en outre une assurance supplémentaire en matière de cybersécurité.

Parce que la technologie Intercept X est si efficace pour stopper les tentatives de violations avant qu'elles ne commencent, la charge de travail EDR est considérablement allégée. Cela signifie que les entreprises informatiques peuvent optimiser leurs ressources clés, leur permettant ainsi de se concentrer sur leurs activités plutôt que de rechercher des faux positifs et de gérer des volumes d'alertes trop importants.

Davantage d'expertise, moins d'effectifs

L'EDR intelligent, intégré au nouvel Intercept X Advanced with EDR de Sophos, reproduit les capacités d'analystes hautement qualifiés, permettant ainsi aux entreprises d'ajouter de l'expertise sans avoir à augmenter leurs effectifs. Contrairement à d'autres solutions EDR faisant appel à des analystes humains hautement qualifiés pour se poser les bonnes questions et interpréter les données, Intercept X Advanced with EDR est basé sur le Machine Learning et est enrichi par des informations sur les menaces issues des SophosLabs.

Expertise en matière de sécurité* : En détectant automatiquement les menaces potentielles et en les classant par ordre de priorité, Intercept X Advanced with EDR met son expertise en matière de sécurité entre les mains des équipes informatiques. Grâce au Machine Learning, les événements suspects sont identifiés et classés dans la catégorie la plus importante, requérant une attention immédiate. Les analystes peuvent rapidement déterminer où concentrer leur attention et identifier les machines touchées.

Expertise sur les malwares : La plupart des entreprises dépendent d'experts en malwares spécialisés dans la rétro-ingénierie pour analyser les fichiers suspects. Cette approche est non seulement chronophage et difficile à réaliser, mais elle suppose un niveau de sophistication en cybersécurité que la plupart des entreprises ne possèdent pas. En s'appuyant sur l'analyse des malwares par Deep Learning, l'approche d'Intercept X Advanced with EDR est bien meilleure. En effet, elle permet d'analyser automatiquement les malwares dans les moindres détails, décomposant les attributs des fichiers et les codes et les comparant à des millions d'autres fichiers. Les analystes peuvent facilement identifier les attributs et segments de code similaires aux fichiers de « bonne réputation » ou de « mauvaise réputation », afin de déterminer si un fichier doit être bloqué ou autorisé.

Expertise en matière d'intelligence sur les menaces : Lorsqu'Intercept X Advanced with EDR classe un fichier potentiellement suspect, les administrateurs informatiques peuvent obtenir plus d'informations en accédant aux données sur les menaces des SophosLabs, qui reçoivent et traitent environ 400 000 nouveaux échantillons de malwares chaque jour. Ces données et d'autres informations sur les menaces sont collectées, rassemblées et résumées afin de faciliter l'analyse. Cela signifie que les équipes ne disposant pas d'analystes spécialisés dans l'intelligence sur les menaces ou n'ayant pas accès à des flux sophistiqués de données sur les menaces peuvent bénéficier de l'une des meilleures équipes de recherche en cybersécurité et en sciences des données au monde.

Réponse guidée aux incidents

Intercept X Advanced with EDR permet aux administrateurs de répondre aux questions complexes soulevées par les incidents de sécurité, en fournissant une visibilité sur la portée d'une attaque, son origine, ce qui a été touché et la manière d'y répondre. Les investigations guidées permettent aux équipes de sécurité, de tous niveaux, de comprendre rapidement leurs postures en matière de sécurité grâce aux instructions contextuelles, qui suggèrent les prochaines étapes à suivre, des représentations visuelles claires des attaques, et une expertise intégrée.

Une fois l'investigation terminée, les analystes peuvent répondre en un clic. Les options d'intervention immédiate incluent la capacité à isoler les terminaux pour un nettoyage immédiat, à nettoyer et à bloquer des fichiers et à créer des instantanés d'analyse.

Scénarios d'utilisation de l'EDR intelligent

La fonctionnalité EDR permet aux équipes de sécurité d'avoir la visibilité et l'expertise dont elles ont besoin pour mieux relever les défis des menaces actuelles les plus complexes, tels que :

- Comprendre la portée et l'impact des incidents de sécurité.
- Détecter les attaques qui peuvent passer inaperçues.
- Rechercher des indicateurs de mise en danger du réseau.
- Prioriser les événements pour permettre une investigation plus poussée.
- Analyser les fichiers pour déterminer s'ils constituent des menaces potentiellement indésirables ou véritables.
- Rendre compte en toute confiance de l'attitude sécurité de l'entreprise, et ce à tout moment.

Au-delà de l'EDR

Pour bloquer la plus grande gamme de menaces, Intercept X Advanced with EDR utilise une approche globale de défense en profondeur plutôt que de s'appuyer simplement sur une technique de sécurité primaire. C'est ce que nous appelons « la puissance du plus », c'est-à-dire une combinaison de techniques de pointe fondamentales et modernes. Intercept X Advanced with EDR intègre la fonctionnalité EDR au sein de la meilleure protection contre les malwares et les exploits du marché.

Les techniques modernes incluent la détection des malwares par Deep Learning, la prévention des exploits et des fonctions spécialement conçues pour bloquer les ransomwares. Les techniques fondamentales incluent un antivirus, l'analyse comportementale, la détection du trafic malveillant, la prévention des pertes de données, et bien plus.

Intercept X Advanced with EDR associe des capacités EDR avec les fonctionnalités modernes présentes dans Intercept X et les techniques fondamentales de Sophos Central Endpoint Protection. Le tout livré sous la forme d'une solution unique, dans un seul agent.

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Intercept X	Sophos Endpoint Protection
Techniques fondamentales	✓	✓		✓
Deep Learning	✓	✓	✓	
Anti-exploit	✓	✓	✓	
CryptoGuard anti-ransomware	✓	✓	✓	
Endpoint detection and response (EDR)	✓			

* Disponible début 2019

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

Essayez-le dès aujourd'hui

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

18-10-02 DS-FR (3098-DD)

SOPHOS