Présentation de la solution

Sophos Endpoint

Prévention des violations, des ransomwares et des fuites de données

Sophos Intercept X est la solution de sécurité Endpoint la plus complète sur le marché, offrant plusieurs couches de sécurité pour une protection inégalée contre les attaques avancées. La solution utilise une approche de défense en profondeur qui bloque la plus large gamme de menaces avant que celles-ci n'aient un impact sur les systèmes. Des outils EDR/XDR puissants permettent aux équipes informatiques et de sécurité de chasser, d'investiguer et de répondre aux menaces.

Cas d'usages

1 | APPROCHE AXÉE SUR LA PRÉVENTION

Résultats souhaités : Arrêter plus de menaces en amont pour minimiser les risques et réduire la charge de travail en matière d'investigation et de réponse.

Solution : Intercept X adopte une approche globale pour protéger tous les postes de travail et ne s'appuie pas uniquement sur une seule technique de sécurité. Le contrôle du Web, des applications et des périphériques réduit la surface d'attaque et bloque les vecteurs d'attaque courants. L'IA, l'analyse comportementale, les technologies anti-ransomware et anti-exploit, ainsi que d'autres technologies de pointe, bloquent rapidement les menaces avant qu'elles ne prennent de l'ampleur.

2 | GESTION OPTIMISÉE

Résultats souhaités : Se concentrer sur la prévention, la détection et la réponse aux menaces plutôt que sur l'administration.

Solution : Sophos Central est une console de gestion Cloud d'où les clients peuvent gérer tous les produits Sophos et lancer des actions de chasse aux menaces et d'investigation. Des paramètres de politique par défaut robustes garantissent la mise à disposition immédiate de paramètres de protection recommandés aux clients, sans nécessiter de formation ou de réglages supplémentaires. La fonction 'Intégrité du compte' dans Sophos Central aide à identifier et à résoudre les problèmes de sécurité.

3 | DÉFENSES CONTEXTUELLES

Résultats souhaités : Des défenses qui s'adaptent automatiquement à mesure que l'attaque évolue.

Solution : Lorsque Intercept X détecte une attaque pilotée manuellement, il active automatiquement des défenses supplémentaires sur le poste de travail avec une approche « Shields Up » pour empêcher l'attaque de se poursuivre. La protection adaptative contre les attaques bloque les activités suspectes, telles que les téléchargements d'outils d'administration à distance, offrant à votre équipe un temps précieux pour répondre à la menace.

4 | DÉTECTION ET RÉPONSE

Résultats souhaités : Détecter et répondre aux menaces qui ne peuvent être maitrisées par la seule protection.

Solution : La puissante fonctionnalité EDR/XDR permet aux clients de chasser, d'investiguer et de répondre aux activités suspectes à l'aide de contrôles de sécurité fournis par Sophos et par des fournisseurs tiers. C'est par exemple le cas des exfiltrations de données ou des adversaires silencieux qui n'utilisent pas de code malveillant. Les clients qui n'ont pas les ressources nécessaires pour gérer la sécurité en interne peuvent faire appel à Sophos MDR pour bénéficier d'une détection et d'une réponse aux menaces 24/7, assurées par une équipe d'experts.

Gartner

Un Leader du Magic Quadrant de Gartner pour les plateformes de protection Endpoint dans 14 rapports consécutifs.

SE Labs

Une protection à la pointe de l'industrie récompensée par des tests indépendants.

THE CHANNEL CO. CRN TECH INNOVATORS 2023

Meilleure sécurité Endpoint aux CRN Tech Innovators Awards (juillet 2023)

Pour en savoir plus et évaluer Sophos Intercept X :
sophos.fr/endpoint

© Copyright 2024. Sophos Ltd. Tous droits réservés. Immatriculée en Angleterre et au Pays de Galles No. 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.

Le logo Gartner Peer Insights est une marque déposée et une marque de service de Gartner, Inc. ou de ses affiliés, et est utilisé ici avec autorisation. Tous droits réservés. Le contenu de Gartner Peer Insights est constitué d'avis d'utilisateurs individuels basés sur leurs propres expériences avec les éditeurs répertoriés sur la plateforme. Ces avis ne doivent pas être interprétés comme des déclarations de faits et ne représentent pas les opinions de Gartner ou de ses affiliés. Gartner ne cautionne aucun fournisseur, produit ou service décrit dans ce contenu et n'offre aucune garantie, explicite ou implicite, quant à l'exactitude ou l'exhaustivité de ce contenu, y compris toute garantie de qualité marchande ou d'adéquation à un usage particulier.

2024-01-15 SB-FR (PC)

SOPHOS