SOPHOS

SOPHOS NDR

Visualisez et bloquez les menaces sur l'ensemble du réseau de l'ère de l'IA.

Une seule solution pour détecter et se défendre contre les menaces connues et inconnues.

Sophos NDR combine l'analyse comportementale optimisée par l'IA et le ML, l'analyse du trafic chiffré, l'analyse réseau et la chasse aux menaces avec l'inspection approfondie des paquets et des capacités IDS/IPS. Les options de déploiement flexibles, la réponse active en ligne et la défense connectée via Sophos Fusion aident les organisations à étendre leur visibilité sur les réseaux hybrides et à surveiller les ressources non gérées et sans agent afin de bloquer les menaces plus rapidement et de renforcer leur défense coordonnée.

77 %

des équipes IT n'ont pas une visibilité totale sur les environnements hybrides[1]

3,4 heures

Délai médian avant que les attaquants ne ciblent Active Directory après avoir obtenu l'accès[2]

3 jours

temps médian avant qu'un attaquant ne soit détecté dans un environnement[2]

CE QUE VOUS OBTENEZ AVEC SOPHOS NDR

Quatre résultats pour une défense réseau renforcée.

Bénéficiez d'une meilleure visibilité sur l'ensemble du réseau.

Obtenez une visibilité au niveau du réseau sur les communications impliquant des ressources gérées, non gérées et sans agent. Identifiez les comportements suspects et les activités d'attaque qui pourraient échapper aux dispositifs de contrôle pris isolément.

- Analyse comportementale pour identifier les comportements suspects sur le réseau
- Visibilité sur les ressources non gérées, IoT, OT et sans agent
- Détection des mouvements latéraux et des communications de commande et de contrôle

Bloquer les menaces plus rapidement.

Réduisez le temps entre détection et réponse. Sur une appliance Sophos NDR dotée du module complémentaire IDS/IPS, le mode Active Inline peut bloquer automatiquement les paquets malveillants connus sur le trajet du trafic réseau.

- Bloquez les paquets malveillants connus en temps réel
- Passez de la surveillance passive à la prévention active en ligne
- Appliquez l'inspection approfondie des paquets et l'IDS/IPS directement sur le chemin du trafic

Choisissez votre mode de déploiement.

Déployez sous forme d'appliance virtuelle, sur du matériel Sophos NDR dédié ou sur du matériel tiers compatible. Adaptez la surveillance et l'application des mesures de sécurité à votre architecture, à vos exigences et à votre tolérance au risque.

- Déploiements virtuels illimités
- Options matérielles adaptées à votre environnement
- Modes de déploiement SPAN/TAP et en ligne adaptés aux exigences opérationnelles

Simplifiez les opérations avec Sophos Fusion.

Intégrez la télémétrie, les détections et le contexte du réseau dans Sophos Fusion, aux côtés des données issues des postes, des pare-feu, des identités, des emails et du cloud, pour faciliter l'investigation et coordonner la réponse.

- Unifiez le contexte réseau avec les informations de Sophos Fusion
- Enrichissez les investigations Sophos MDR et XDR avec la télémétrie NDR
- Coordonnez la détection et la réponse dans l'ensemble du système de défense Sophos Fusion

SOPHOS NDR EN UN COUP D'ŒIL

- Les analyses comportementales basées sur l'IA et le ML détectent les menaces inconnues et évasives
- L'inspection approfondie des paquets et les capacités IDS/IPS éprouvées permettent d'identifier les menaces connues
- Blocage actif en ligne du trafic malveillant connu
- Options de déploiement virtuel, sur matériel Sophos dédié ou sur matériel tiers compatible

À QUI S'ADRESSE SOPHOS NDR

- Organisations cherchant à combler les lacunes en matière de visibilité réseau
- Les équipes de sécurité à la recherche de visibilité sur les ressources non gérées et sans agent
- Organisations nécessitant un déploiement NDR flexible sur des réseaux diversifiés et distribués
- MSP et MSSP qui développent leurs services de surveillance des réseaux, de chasse aux menaces et de sécurité gérée

VOTRE AVANTAGE CONTRE LES MENACES RÉSEAU

Détection comportementale et prévention active réunies.

Couverture de détection plus large

Les attaquants peuvent exploiter les failles de visibilité sur les réseaux hybrides, appareils non gérés et ressources sans agent. Sophos NDR combine l'analyse comportementale, l'analyse du trafic chiffré, la chasse aux menaces, l'inspection approfondie des paquets et l'IDS/IPS pour détecter les menaces connues et inconnues.

Bloquez directement les menaces sur le trajet du trafic réseau

La détection seule peut amener les équipes de sécurité à réagir alors que le trafic malveillant a déjà atteint sa destination. Sur une appliance Sophos NDR dotée du module complémentaire IDS/IPS, le mode Active Inline inspecte le trafic en temps réel et bloque automatiquement les paquets malveillants connus sur le trajet du trafic réseau.

Défense connectée avec Sophos Fusion

Les menaces réseau existent rarement de manière isolée. Sophos NDR apporte la télémétrie réseau, les détections et le contexte à Sophos Fusion, aidant les équipes à accélérer les investigations et à coordonner la réponse sur l'ensemble du système de défense.

CE QUE DISENT NOS CLIENTS

« Dans l'ensemble, mon expérience avec Sophos NDR a été plutôt bonne. Il aide grandement à obtenir une visibilité sur les comportements anormaux du réseau et à détecter des schémas qui passeraient normalement inaperçus dans la surveillance traditionnelle. J'apprécie vraiment le fait que les alertes soient claires et faciles à interpréter, ce qui accélère l'analyse et la prise de décision. »[3]

Sécurité informatique et gestion des risques, secteur bancaire — Gartner® Peer Insights™

SOPHOS FUSION

Un seul système. Tous les points de contrôle. Une défense unifiée.

Sophos NDR fait partie de Sophos Fusion, le système de cyberdéfense le plus complet sur le marché. Il protège votre organisation contre les menaces accélérées par l'IA qui évoluent plus rapidement que ne peuvent réagir les défenseurs.

sophos.com/NDR →

[1] SolarWinds, rapport 2026 sur l'état de la surveillance et de l'observabilité

[2] Sophos, rapport Sophos Active Adversary 2026

[3] https://www.gartner.com/reviews/market/network-detection-and-response/vendor/sophos/product/sophos-ndr/review/view/6513218

Le contenu de Gartner Peer Insights est constitué d'avis d'utilisateurs individuels basés sur leurs propres expériences et ne doit pas être interprété comme des déclarations de faits et ne représente 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.

Gartner® et Peer Insights™ sont des marques commerciales de Gartner, Inc. et/ou de ses filiales. Tous droits réservés.

© Copyright 2026. 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 d'entreprises mentionnés dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

2026-10-23 SB-FR (TA)

SOPHOS