Sophos Network Detection and Response

Un complément puissant pour Sophos XDR et Sophos MDR

Sophos NDR fonctionne avec vos solutions endpoint et pare-feu pour surveiller l'activité du réseau et détecter les schémas suspects et malveillants invisibles à leurs yeux. Sophos NDR détecte les flux de trafic inhabituels provenant de systèmes non gérés et d'appareils connectés (IoT), d'actifs indésirables, de menaces internes, d'attaques zero-day inédites et de modèles inhabituels en profondeur dans le réseau.

Sophos NDR fournit une visibilité essentielle sur l'activité du réseau que d'autres produits ne perçoivent pas

Les attaquants sont doués pour échapper à la détection, mais toute attaque a besoin de se déplacer sur le réseau. Sophos NDR détecte les modèles de trafic réseau suspects qui ne sont pas identifiés par vos solutions endpoint et pare-feu, notamment :

- **Appareils réseau inconnus ou non protégés** : y compris les appareils IoT ou OT légitimes qui ne peuvent pas être entièrement gérés avec un capteur endpoint, ainsi que les systèmes inconnus ou non identifiés sur le réseau. Ces appareils peuvent être compromis ou le devenir lors d'une attaque. Sophos NDR identifie et surveille ces appareils pour détecter tout comportement suspect ou malveillant qui pourrait signaler une attaque.
- **Actifs non autorisés ou indésirables** : les actifs introduits sur le réseau qui peuvent déjà être compromis ou utilisés pour lancer une attaque peuvent être facilement identifiés et surveillés par Sophos NDR.
- **Activité 'Command and Control' (C2) nouvelle ou précédemment invisible** : de nombreuses attaques ou violations sont orchestrées à distance en utilisant ce qui semble être des communications légitimes entre un acteur malveillant et ses processus distants à l'intérieur du réseau. Sophos NDR peut détecter de nouvelles activités C2 de type zero-day pour identifier une attaque ciblée qui vient juste d'être lancée.
- **Flux et modèles de trafic réseau suspects ou malveillants** : il peut s'agir de signaux importants dans l'identification précoce d'une cyberattaque. Les indicateurs peuvent inclure les activités réseau ou accès à distance inhabituels en dehors des heures de bureau, les téléchargements ou exfiltrations de données suspects, les modèles de trafic anormaux et du trafic malveillant généré par des malwares connus.

Sophos NDR collabore avec votre pare-feu

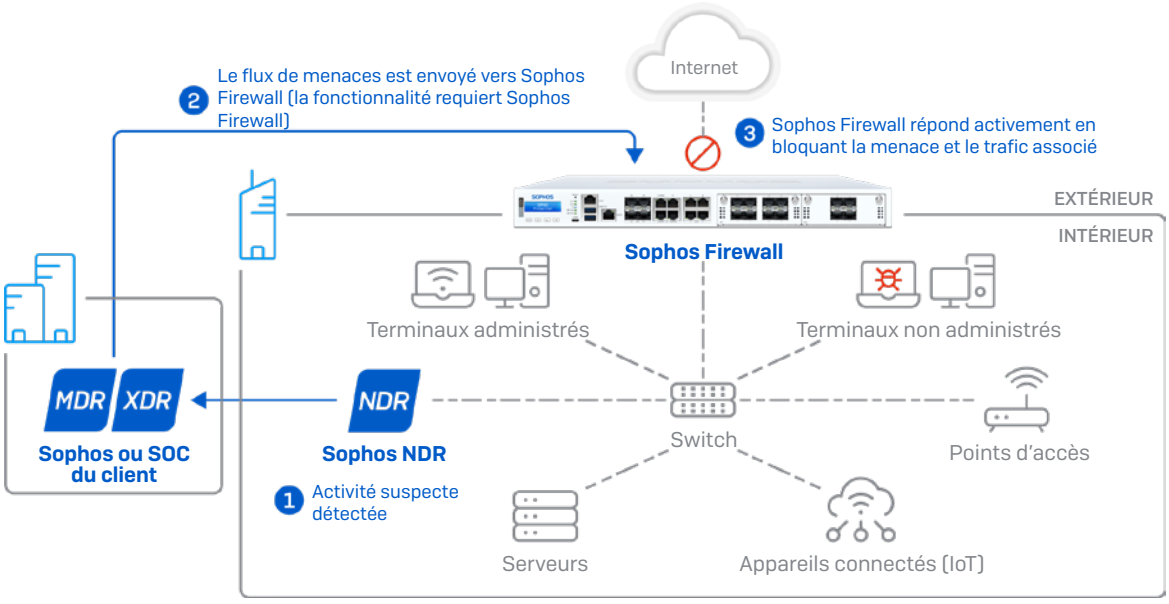
Les pare-feux jouent un rôle essentiel dans la sécurisation du périmètre de votre réseau et dans le contrôle de ce qui y entre et en sort. Sophos NDR est le complément parfait de votre solution de pare-feu, car ils travaillent ensemble pour fournir des informations et une protection à l'intérieur du réseau, là où votre pare-feu manque de visibilité. Il inclut également des technologies qui identifient de façon unique les activités suspectes et malveillantes qui traversent votre réseau interne et qui ne peuvent pas être détectées par un pare-feu ou un produit de protection Endpoint.

Avantages principaux

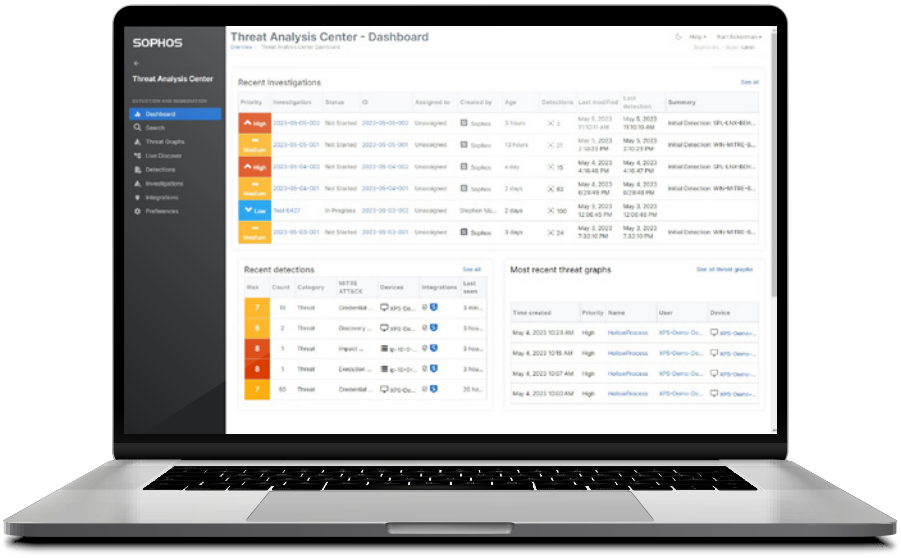
- Complément idéal de Sophos XDR et MDR, permettant des détections en profondeur au sein d'un réseau.
- Fonctionne avec votre pare-feu pour détecter les activités et les menaces sur le réseau.
- Détecte les activités réseau suspectes provenant d'appareils inconnus ou non gérés, d'actifs indésirables et de serveurs C2 zero-day.
- Inspecte les flux de trafic chiffrés sans compromettre les informations confidentielles.
- Déploiement, configuration et gestion à partir de Sophos Central.
- Utilisez la console d'investigation pour obtenir des informations sur les activités suspectes du réseau et analyser ou investiguer les modèles anormaux.

SOPHOS

Sophos NDR opère en profondeur au sein de votre réseau pour détecter les attaques

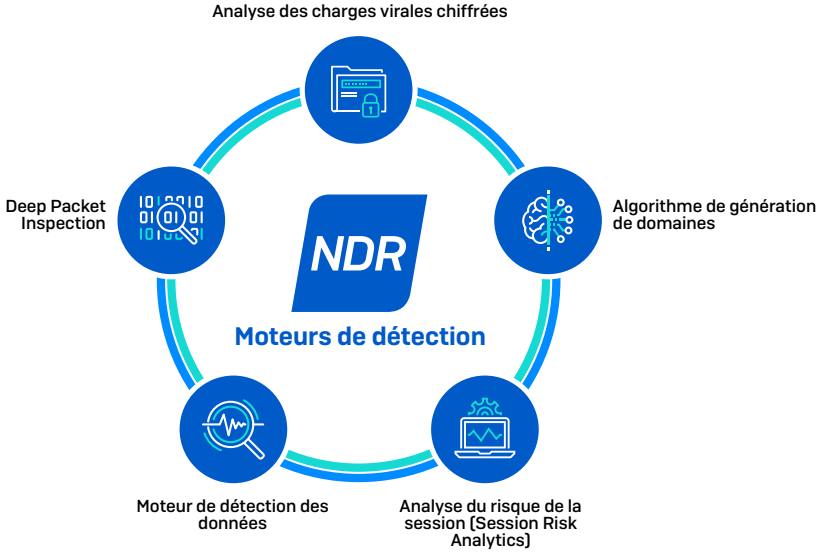


- Il surveille le trafic au cœur d'un réseau à l'aide de cinq moteurs en temps réel.
- Il détecte l'activité de tous les actifs sur le réseau, y compris les systèmes non gérés, les appareils IoT et les actifs indésirables, en identifiant le fabricant et le système d'exploitation, ainsi que tout modèle de trafic suspect provenant de ces appareils.
- Il alimente en données et en alertes le Data Lake de Sophos Central, l'équipe Sophos MDR ou votre propre équipe XDR.
- Obtenez une visibilité et des informations sur l'activité du réseau et des applications, les flux à risque et le trafic suspect grâce à une console d'investigation facile à utiliser.
- Si vous avez Sophos Firewall, la réponse automatisée aux menaces est disponible pour bloquer immédiatement les menaces et empêcher les mouvements latéraux.
- Fonctionne en tant qu'appliance virtuelle sur les plateformes d'hyperviseurs les plus courantes comme VMware et Hyper-V.
- Il se connecte directement à votre switch via le miroir de port SPAN pour surveiller l'ensemble du trafic
- Il inspecte les données chiffrées des paquets sans compromettre les données personnelles identifiables



Moteurs de détection de Sophos NDR

Sophos NDR comprend cinq moteurs de détection qui analysent en continu les flux de trafic réseau et appliquent l'analyse par Machine Learning/IA pour identifier les activités suspectes et malveillantes au sein de votre réseau.



Moteurs de détection	Description
Analyse des charges virales chiffrées (EPA)	Le moteur détecte les serveurs C2 de type zero-day et les nouvelles variantes des familles de malwares en se basant sur les modèles de comportement trouvés dans la taille, la direction et les temps interarrivés des sessions.
Algorithme de génération de domaines (DGA)	Le moteur identifie la présence d'une technologie dynamique de génération de domaines utilisée par les logiciels malveillants pour éviter la détection.
Inspection approfondie des paquets (DPI)	Le moteur DPI surveille le trafic chiffré et non chiffré en utilisant des IOC connus pour identifier rapidement les menaces et les TTP.
Analyse du risque de la session (SRA)	Un puissant moteur logique qui utilise des règles alertant sur une multitude de facteurs de risque basés sur la session.
Moteur de détection des appareils (DDE)	Un moteur de requête extensible qui utilise un modèle de prédiction par Deep Learning pour analyser le trafic chiffré et identifier des modèles de comportement parmi des flux de réseau non apparentés et détecter l'analyse des ports et l'activité de force brute au niveau du SSH.

Licences Sophos NDR

Sophos NDR est le complément parfait de Sophos XDR et Sophos MDR, et est disponible sous forme de pack d'intégration. La tarification de Sophos NDR est basée sur le nombre total d'utilisateurs et de serveurs de l'entreprise. Le logiciel de l'appliance virtuelle est inclus dans la licence, et vous pouvez déployer autant de capteurs NDR que nécessaire. Ce qui est plus abordable et plus souple que les offres concurrentes facturées à l'unité.

Spécifications techniques de Sophos NDR

Plateformes prises en charge

- VMware ESXi6.7 et versions ultérieures
- Microfost Hyper-V 6.0.600118016 (Windows Server 2016) ou version ultérieure
- Amazon AWS c5n.2xlarge
- Matériel certifié

Matériel	Débit max.	Connexions max./sec	CPU	Mémoire
Dell R660 (2 prises)	40 Gbit/s	120 000	64	128 Go
Dell R660 (1 prise)	40 Gbit/s	80 000	32	64 Go
Dell R650	20 Gbit/s	40 000	24	64 Go
Dell R450	10 Gbit/s	20 000	16	32 Go
Dell R350	4 Gbit/s	8 000	8	32 Go
Intel Nuc 13th Gen	2,5 Gbit/s	4 000	12	32 Go

Configuration système requise pour les VM

Les VM Sophos NDR prennent en charge jusqu'à 1 Gbit/s par capteur :

- Utilisez les paramètres de VM par défaut pour les volumes de trafic moyens :
  - Jusqu'à 500 Mbit/s
  - Jusqu'à 70 000 paquets/sec
  - Jusqu'à 1 200 flux/sec
- Redimensionnez la VM à 8 vCPU pour des volumes de trafic élevés :
  - Jusqu'à 1 Gbit/s
  - Jusqu'à 300 000 paquets/sec
  - Jusqu'à 4 500 flux/sec

Ressources supplémentaires :

- Ressources de la communauté Sophos NDR
- Améliorez vos opérations de sécurité avec Sophos Network Detection and Response (NDR)
- Spécifications du matériel certifié

Pour en savoir plus :

sophos.fr/ndr

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

24-12-19 DS-FR (MP)

SOPHOS