Brochure de la solution

Sophos Extended Detection and Response

Se défendre contre les adversaires actifs avec des fonctionnalités EDR et XDR complètes

Il est essentiel de stopper rapidement les attaques. Sophos XDR (Extended Detection and Response) fournit des outils et des renseignements sur les menaces puissants qui vous permettent de détecter, d'investiguer et de répondre aux activités suspectes sur l'ensemble de votre environnement IT.

Conçu à partir de la protection Endpoint la plus robuste

Les équipes informatiques ont moins d'incidents à investiguer et à résoudre lorsque davantage de menaces sont stoppées en amont. Sophos associe des fonctionnalités XDR à la protection Endpoint la plus robuste sur le marché, pour bloquer les menaces avant qu'elles ne nécessitent une investigation manuelle — allégeant ainsi votre charge de travail.

Solution EDR intégrée

Sophos XDR inclut des outils EDR (Endpoint Detection and Response) complets, y compris des capacités de recherche puissantes et personnalisables comprenant l'accès à 90 jours de données sur les postes et les serveurs, ainsi qu'un accès à distance sécurisé aux appareils. Investiguez les incidents, installez/désinstallez des logiciels, arrêtez des processus, etc.

Étendez la visibilité au-delà de vos postes

Plus votre visibilité sera large, plus vite vous pourrez agir. Les événements issus des produits Sophos et non Sophos sont ingérés, filtrés, corrélés et priorisés. Cela étend la visibilité sur toutes les surfaces d'attaque clés et vous permet de détecter et de bloquer rapidement les adversaires actifs.

Vaste portefeuille de solutions compatibles Sophos XDR

Les technologies Sophos travaillent ensemble de manière transparente dans la plateforme XDR pour fournir les meilleurs résultats possibles en matière de sécurité. Les intégrations de solutions natives incluent Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos NDR, Sophos ZTNA, Sophos Email et Sophos Cloud.

Compatible avec vos outils et vos technologies existants

Exploitez la télémétrie d'un large éventail d'outils de sécurité non Sophos et obtenez un meilleur retour sur investissement de vos technologies existantes tout en accélérant les opérations de sécurité. Les intégrations incluent les technologies de gestion des identités, de réseau, de pare-feu, de messagerie, de plateforme Cloud, de productivité et de sécurité Endpoint.

Avantages principaux

- Vous obtenez une visibilité sur les activités suspectes sur toutes les surfaces d'attaque clés
- Une plateforme XDR unifiée avec une gamme étendue de solutions Sophos intégrées
- Exploitez les outils et les investissements existants grâce à des intégrations technologiques non Sophos étendues
- Investiguez et répondez rapidement aux menaces grâce à des détections priorisées par l'IA et des flux de travail optimisés
- La solution inclut une protection Endpoint et des fonctionnalités EDR de pointe

Accélérez la détection, l'investigation et la réponse

Sophos XDR inclut des outils et des fonctionnalités conçus pour accroître la productivité des analystes de sécurité et des administrateurs informatiques. Les investigations guidées par l'IA vous permettent de comprendre rapidement l'étendue et la cause d'un incident, et de minimiser le temps de réponse.

Des détections priorisées par l'IA sur toutes les surfaces d'attaque clés

Identifiez aisément les activités suspectes qui nécessitent une attention immédiate. Sophos XDR priorise automatiquement les détections en fonction du risque et fournit un contexte complet.

Mappage au cadre MITRE ATT&CK

Les détections et les dossiers sont automatiquement mappés aux tactiques de MITRE ATT&CK, pour vous permettre d'identifier facilement les failles dans les défenses et prioriser les améliorations.

Investiguez et chassez les menaces rapidement

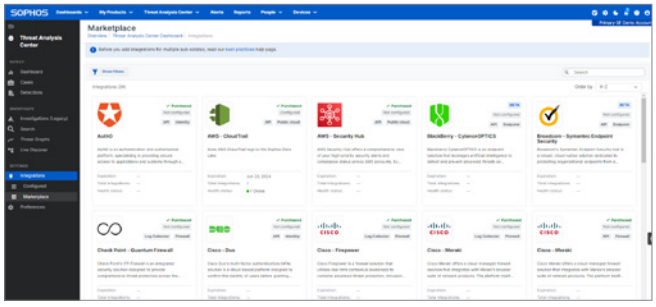
Des outils de recherche puissants, dont des modèles de requête préétablis, vous permettent de trouver plus rapidement les données dont vous avez besoin, sans avoir besoin d'être un expert en SQL.

Réponse automatisée et accélérée

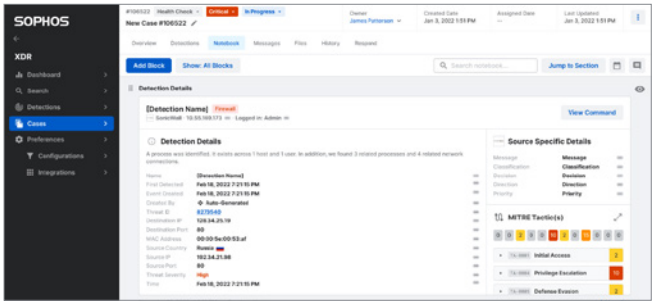
Les actions automatisées, telles que l'arrêt des processus, la restauration des fichiers touchés par un ransomware et l'isolement du réseau, permettent de contenir rapidement les menaces et de gagner un temps précieux.

Gestion collaborative des dossiers

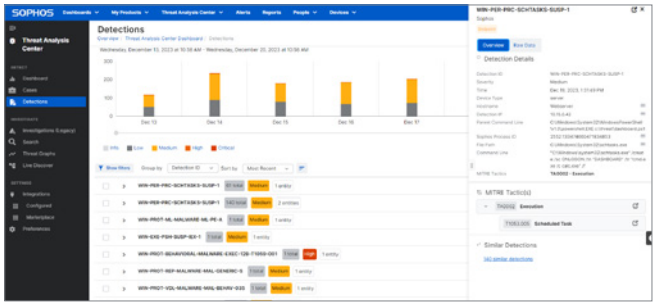
La création automatique de dossiers permet d'accélérer les investigations, et des outils de gestion complets favorisent la collaboration entre membres de l'équipe.



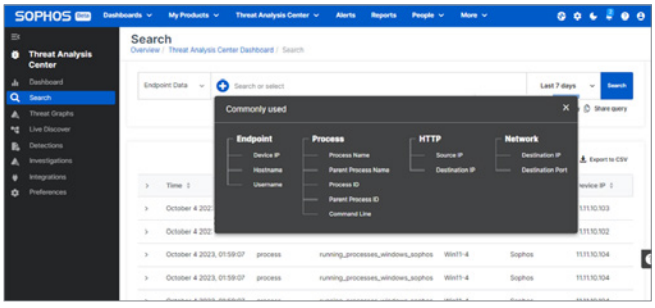
Compatible avec les solutions Sophos et tierces



Des outils puissants de gestion de dossiers et de collaboration



Des détections priorisées par l'IA sur toutes les surfaces d'attaque clés



Recherche simple et puissante — aucune expertise SQL n'est nécessaire

Intégrations incluses avec Sophos XDR

Les données de sécurité provenant des sources suivantes peuvent être intégrées sans frais supplémentaires avec la plateforme Sophos XDR. Les sources de télémétrie sont utilisées pour élargir la visibilité sur votre environnement, générer de nouvelles détections de menaces et améliorer la fidélité des détections existantes, chasser les menaces, et activer des capacités de réponse supplémentaires.

Ep Sophos Endpoint

Bloquez les menaces avancées et détectez les comportements malveillants sur tous vos postes de travail.

Produit inclus dans le prix de Sophos XDR.

WP Workload Protection

Protection avancée et détection des menaces pour les serveurs et conteneurs Windows et Linux.

Produit inclus dans le prix de Sophos XDR.

Mob Sophos Mobile

Protégez vos appareils iOS et Android et les données qu'ils contiennent contre les dernières menaces mobiles.

Produit vendu séparément ; intégré sans frais supplémentaires.

Fw Sophos Firewall

Surveillez et filtrez le trafic réseau entrant et sortant pour bloquer les menaces avancées avant qu'elles n'aient la possibilité de nuire.

Produit vendu séparément ; intégré sans frais supplémentaires.

Em Sophos Email

Protégez votre boîte de réception contre les malwares avec l'IA avancée pour bloquer les usurpations d'identité et les attaques de phishing.

Produit vendu séparément ; intégré sans frais supplémentaires.

Cld Sophos Cloud

Bloquez les violations du Cloud et obtenez une visibilité accrue sur vos services Cloud critiques, notamment AWS, Azure et GCP.

Produit vendu séparément ; intégré sans frais supplémentaires.

ZT Sophos ZTNA

Remplacez l'accès à distance VPN par un accès à moindre privilège pour connecter en toute sécurité vos utilisateurs à vos applications en réseau.

Produit vendu séparément ; intégré sans frais supplémentaires.

Protection Endpoint tierce

Compatible avec :

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- BlackBerry (Cylance)
- Broadcom (Symantec)

+ compatible avec d'autres solutions dotées de l'agent Sophos 'XDR Sensor'

Outils de Sécurité Microsoft

- Defender for Endpoint
- Defender for Cloud
- Defender for Cloud Apps
- Defender for Identity
- Microsoft Entra ID
- Azure Sentinel
- Office 365 Security and Compliance Center

Conservation des données pendant 90 jours

Conserve les données des produits Sophos et des solutions tierces (non Sophos) dans le Sophos Data Lake.

Prolongeable jusqu'à 1 an avec une option complémentaire.

Journaux d'audit de Microsoft

Fournit des informations sur les actions et les événements des utilisateurs, administrateurs, systèmes et politiques de sécurité ingérées via l'API 'Activité de gestion Office 365'.

Google Workspace

Ingère la télémétrie de sécurité à partir de l'API du Centre d'alerte de Google Workspace.

Intégrations complémentaires

Les données de sécurité provenant des sources suivantes peuvent être intégrées avec la plateforme Sophos XDR en achetant des packs d'intégration. Les sources de télémétrie sont utilisées pour élargir la visibilité sur votre environnement, générer de nouvelles détections de menaces et améliorer la fidélité des détections existantes, chasser les menaces, et activer des capacités de réponse supplémentaires.

Sophos NDR

Surveillez en permanence les activités à l'intérieur de votre réseau pour détecter les actions suspectes qui se produisent entre les appareils et qui ne sont pas visibles autrement.

Compatible avec n'importe quel réseau via le miroir de port SPAN.

Pare-feu

Compatible avec :

- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- Palo Alto Networks
- SonicWall
- WatchGuard

Réseau

Compatible avec :

- Darktrace
- Secutec
- Thinkst Canary
- Skyhigh Security

Gestion d'identité

Compatible avec :

- Auth0
- Duo
- ManageEngine
- Okta

Intégration Microsoft incluse sans frais supplémentaires

Messagerie

Compatible avec :

- Proofpoint
- Mimecast

Intégrations Microsoft 365 et Google Workspace incluses sans frais supplémentaires.

Cloud public

Compatible avec :

- AWS Security Hub
- AWS CloudTrail
- Orca Security

Intégration de données supplémentaires AWS, Azure et GCP via le produit Sophos Cloud, vendu séparément.

Sauvegarde et restauration

Compatible avec :

- Veeam

Conservation des données pendant 1 an

Conserve les données des produits Sophos et des solutions tierces (non Sophos) dans le Sophos Data Lake.

Basé sur la meilleure protection Endpoint sur le marché

Ciblez plus efficacement vos investigations en bloquant davantage d'incidents de sécurité à la source. La plupart des produits XDR obligent les analystes à sacrifier un temps précieux à investiguer des incidents que leur protection aurait dû bloquer en premier lieu. Sophos associe des fonctionnalités XDR à la protection Endpoint la plus robuste sur le marché, pour bloquer les menaces avant qu'elles ne nécessitent une investigation manuelle — allégeant ainsi votre charge de travail.

Les abonnements Sophos XDR incluent Sophos Intercept X Endpoint, offrant une technologie anti-ransomware et anti-exploit avancée, une protection antimalware optimisée par l'IA et des défenses contextuelles qui adaptent le niveau de protection de manière dynamique.

Pour en savoir plus : sophos.fr/endpoint

Un service de détection et de réponse entièrement managé

Choisissez de détecter et d'investiguer les menaces vous-même avec Sophos XDR ou de libérer votre personnel avec un service managé complet 24/7. Avec Sophos Managed Detection and Response (MDR), notre équipe de chasseurs de menaces et d'experts peut vous fournir un centre d'opérations de sécurité (SOC) instantané, y compris des capacités complètes de réponse aux incidents.

Pour en savoir plus : sophos.fr/mdr

Inclus dans les abonnements Sophos XDR

	Sophos XDR
Détections priorisée par l'IA et investigations guidées	✓
Gestion de dossiers, collaboration et actions de réponse	✓
Outils de recherche simples et puissants pour la chasse et l'investigation	✓
Solutions Sophos Endpoint et Workload Protection (Intercept X Advanced)	✓
Outils EDR (Endpoint Detection and Response)	✓
Conservation des données dans le Cloud	90 jours (prolongeable jusqu'à 1 an)
Données riches sur les postes et les serveurs pour EDR	✓
Intégrations avec les solutions Sophos : Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos ZTNA, Sophos Email, Sophos Cloud	✓
Sophos Network Detection and Response (NDR)	Complément en option
Intégrations avec des solutions de protection Endpoint non Sophos	✓
Intégrations avec les solutions Microsoft	✓
Intégration avec la solution de productivité Google Workspace	✓
Intégrations avec des solutions non Sophos de pare-feu, réseau, messagerie, Cloud, identité, sauvegarde et récupération.	Compléments en option

Découvrez pourquoi les clients choisissent Sophos XDR

Sophos est un leader établi en matière de capacités XDR, avec de multiples reconnaissances de l'industrie à l'appui.

Gartner

Sophos a été nommé Leader dans le Magic Quadrant™ 2023 de Gartner® dans la catégorie EPP (Endpoint Protection Platforms) dans 14 rapports consécutifs

Gartner Peer Insights Customers' Choice 2023

Sophos est le seul éditeur reconnu comme Customers' Choice dans les catégories EPP, MDR, Firewall et Mobile Threat Defense

G2 Leader

G2 désigne Sophos comme Leader dans les catégories Endpoint Protection, EDR, XDR, Firewall et MDR dans ses rapports Winter 2024

OMDIA

Sophos était l'éditeur le mieux classé et le seul Leader dans le rapport Omdia Universe for Comprehensive XDR en 2023

MITRE ATT&CK

Sophos a obtenu des résultats exceptionnels dans l'évaluation 2023 de MITRE Engenuity ATT&CK

SE Labs

Sophos obtient régulièrement les meilleurs résultats en matière de protection dans les tests indépendants

Essai gratuit

Évaluation gratuite de 30 jours
sur sophos.fr/xdr

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

2024-02-01 DS-FR (NP)

SOPHOS