Sophos Managed Detection and Response

Détection et réponse aux menaces 24 h/24, 7 j/7

Sophos MDR est un service entièrement managé, disponible 24 h/24 et 7 j/7, fourni par des experts qui détectent et répondent aux cyberattaques ciblant vos ordinateurs, vos serveurs, vos réseaux, vos charges de travail dans le Cloud, vos comptes de messagerie, et bien plus encore.

Services de prévention des ransomwares et des violations

Il est aujourd'hui impératif d'assurer des opérations de sécurité à toute heure du jour et de la nuit. Toutefois, la plupart des entreprises peinent de plus en plus à gérer seules la détection et la réponse aux incidents, car les environnements opérationnels modernes sont devenus trop complexes et les cybermenaces trop rapides.

Avec Sophos MDR, notre équipe d'experts bloque les attaques humaines avancées. Nous prenons les devants pour neutraliser les menaces avant qu'elles ne puissent perturber vos opérations commerciales ou compromettre vos données sensibles. Sophos MDR est personnalisable avec différents niveaux de service, et peut être fourni en utilisant au choix notre technologie propriétaire ou vos outils de cybersécurité existants.

Cybersécurité fournie sous forme de service

Grâce à ses capacités XDR (Extended Detection and Response), qui couvrent tous vos besoins de sécurité partout où se trouvent vos données, Sophos MDR peut :

- **Détecter plus de cybermenaces que les outils de sécurité ne peuvent en identifier à eux seuls**
  Nos outils bloquent automatiquement 99,98 % des menaces, ce qui permet à nos analystes de se concentrer sur la chasse aux attaquants les plus sophistiqués, ceux qui ne peuvent être détectés et bloqués que par un expert hautement qualifié.
- **Agir à votre place pour empêcher les menaces de perturber vos activités**
  Nos analystes détectent, investiguent et répondent aux menaces en quelques minutes, que vous ayez besoin d'un service de réponse aux incidents complet ou d'une simple aide pour prendre des décisions précises.
- **Identifier la cause profonde des menaces afin de prévenir de futurs incidents**
  Nous prenons des mesures proactives et fournissons des recommandations qui réduisent les risques pour votre entreprise. Moins d'incidents signifient moins de perturbations pour vos équipes informatiques et de sécurité, vos employés et vos clients.

Compatible avec les outils de cybersécurité que vous possédez déjà

Nous vous fournissons les technologies dont vous avez besoin grâce à notre vaste portefeuille de solutions primées, mais nos analystes peuvent aussi utiliser vos technologies de cybersécurité existantes pour détecter et répondre aux menaces.

Sophos MDR est compatible avec les données de télémétrie de solutions tierces, dont Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace et bien d'autres encore. La télémétrie est automatiquement consolidée, corrélée et priorisée avec les informations provenant de l'écosystème de cybersécurité adaptatif Sophos ACE et de l'unité de renseignement sur les menaces Sophos X-Ops.

Avantages principaux

- Bloquez les ransomwares et autres attaques avancées pilotées par des humains grâce à une équipe d'experts en réponse aux menaces, disponible 24 h/24 et 7 j/7.
- Optimisez le retour sur investissement de vos technologies de cybersécurité existantes.
- Laissez Sophos MDR exécuter un service complet de réponse aux incidents, travailler avec vous pour gérer les incidents de sécurité ou envoyer des notifications et des conseils détaillés pour remédier aux menaces.
- Améliorez votre éligibilité à une couverture de cyberassurance grâce à la surveillance 24 h/24 et 7 j/7, et aux capacités EDR (Endpoint Detection and Response).
- Libérez votre personnel informatique et de sécurité interne pour qu'il se concentre sur l'activité de votre entreprise.

SOPHOS

Un service MDR qui s'adapte à vous

Sophos MDR est personnalisable avec différents niveaux de service et options de réponse aux menaces. L'équipe Sophos MDR peut au choix exécuter une réponse aux incidents complète, travailler avec vous pour gérer les cyber menaces ou avertir vos équipes de sécurité interne dès que des menaces sont détectées. Notre équipe détermine rapidement les 'qui', 'quoi', 'quand' et 'comment' d'une attaque. Nous pouvons répondre aux menaces en quelques minutes.

Capacités clés

Surveillance et réponse aux menaces 24 h/24, 7 j/7

Nous détectons et répondons aux menaces avant qu'elles ne puissent compromettre vos données ou entraîner des temps d'arrêt. Soutenu par six centres d'opérations de sécurité (SOC) dans le monde, Sophos MDR offre une couverture 24 heures sur 24.

Compatible avec les outils de sécurité non Sophos

Sophos MDR peut intégrer des données de télémétrie provenant de technologies de sécurité tierces (endpoint, pare-feu, identité, messagerie, etc.) dans le cadre de l'écosystème de cybersécurité adaptatif Sophos ACE.

Réponse complète aux incidents

Lorsque nous identifions une menace active, l'équipe Sophos MDR peut exécuter un ensemble complet d'actions de réponse en votre nom et à distance pour intercepter, contenir et éliminer complètement l'adversaire.

Rapports hebdomadaires et mensuels

Sophos Central est votre tableau de bord unique pour les alertes en temps réel, le reporting et la gestion. Les rapports hebdomadaires et mensuels fournissent un aperçu des investigations, des cybermenaces et de votre posture de sécurité.

Écosystème de cybersécurité adaptatif Sophos ACE

Sophos ACE bloque automatiquement les activités malveillantes et nous permet de rechercher les signaux faibles des menaces que seule une intervention humaine peut détecter, investiguer et éliminer.

Chasse aux menaces dirigée par des experts

Les chasses aux menaces proactives effectuées par des analystes hautement qualifiés permettent de découvrir et d'éliminer rapidement plus de menaces que les produits de sécurité seuls ne peuvent détecter. L'équipe Sophos MDR peut également utiliser la télémétrie de fournisseurs tiers pour chasser les menaces et identifier les comportements des attaquants qui ont échappé à la détection des outils déployés.

Assistance téléphonique directe

Votre équipe a un accès direct par téléphone à notre centre d'opérations de sécurité (SOC) pour examiner les menaces et les incidents actifs. L'équipe Sophos MDR est disponible 24 h/24, 7 j/7 et 365 j/an, et s'appuie sur nos équipes du support technique réparties sur 26 sites dans le monde entier.

Interlocuteur dédié en cas d'incident

Vous avez un accès direct à un responsable de la réponse aux incidents qui collabore avec votre équipe interne et vos partenaires externes dès que nous identifions un incident et travaille avec vous jusqu'à la résolution de l'incident.

Analyse détaillée des attaques (RCA)

En plus de fournir des recommandations proactives pour améliorer votre sécurité, nous effectuons une analyse détaillée des attaques (RCA) pour identifier les problèmes sous-jacents qui ont conduit à un incident. Nous vous donnons des conseils prescriptifs pour remédier aux failles de sécurité afin qu'elles ne soient pas exploitées à l'avenir.

Fonction « Vérifier l'état du compte » de Sophos

Nous examinons en continu les paramètres et les configurations des systèmes endpoints gérés par Sophos XDR et nous nous assurons qu'ils fonctionnent à un niveau optimal.

Confinement des menaces

Pour les entreprises qui choisissent de ne pas confier à Sophos MDR le service complet de réponse aux incidents, l'équipe Sophos MDR peut exécuter des actions de confinement des menaces, interceptant la menace et empêchant sa propagation. Cela réduit la charge de travail des équipes de sécurité internes et leur permet d'exécuter rapidement des actions de remédiation.

Briefing de renseignement : « Sophos MDR ThreatCast »

Fourni par l'équipe Sophos MDR, le « Sophos MDR ThreatCast » est un briefing mensuel disponible exclusivement pour les clients de Sophos MDR. Il fournit un aperçu des derniers renseignements sur les menaces collectés et des bonnes pratiques de sécurité.

Sophos Breach Protection Warranty

La garantie Sophos Breach Protection Warranty est incluse dans toutes les licences Sophos MDR Complete annuelles (un à cinq ans) et mensuelles. Elle couvre jusqu'à 1 million de dollars (USD) de frais de réponse aux incidents. Il n'y a pas de niveaux de garantie, de durée minimale de contrat ou de conditions d'achat supplémentaires.

Niveaux de service de Sophos

	Sophos Threat Advisor	Sophos MDR	Sophos MDR Complete
Surveillance et réponse aux menaces par des experts, 24 h/24 et 7 j/7	✓	✓	✓
Compatible avec les produits de sécurité non Sophos	✓	✓	✓
Rapports hebdomadaires et mensuels	✓	✓	✓
Briefing de renseignement mensuel : « Sophos MDR ThreatCast »	✓	✓	✓
Fonction « Vérifier l'état du compte » de Sophos		✓	✓
Chasse aux menaces dirigée par des experts		✓	✓
Confinement des menaces : les attaques sont interceptées, bloquant leur propagation Utilise l'agent complet Sophos XDR (protection, détection et réponse) ou Sophos XDR Sensor (détection et réponse)		✓	✓
Assistance téléphonique directe pendant les incidents actifs		✓	✓
Service complet de réponse aux incidents : les menaces sont entièrement éliminées Requiert l'agent complet Sophos XDR (protection, détection et réponse)			✓
Analyse détaillée des attaques (RCA)			✓
Interlocuteur dédié en cas d'incident			✓
Sophos Breach Protection Warranty Couvre jusqu'à 1 million de dollars (USD) de frais de réponse			✓

Intégrations incluses avec Sophos MDR

Les données de sécurité provenant des sources suivantes peuvent être intégrées sans frais supplémentaires pour être utilisées par l'équipe Sophos MDR. 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, mener des chasses aux menaces et activer des capacités de réponse supplémentaires.

Sophos XDR

La seule plateforme XDR qui combine des intégrations natives pour les solutions endpoint, serveur, pare-feu, Cloud, messagerie, mobiles et Microsoft.

Inclus dans le prix de Sophos MDR et Sophos MDR Complete

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.

Microsoft Graph Security

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Identity Protection (Azure AD)
- Microsoft Azure Sentinel
- Office 365 Security and Compliance Center
- Azure Information Protection

Sophos Endpoint

Bloquez les menaces avancées et détectez les comportements malveillants, y compris les attaquants qui se font passer pour des utilisateurs légitimes.

Inclus dans le prix de Sophos MDR et Sophos MDR Complete

Sophos Email

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

Produit vendu séparément ; intégré sans frais supplémentaires.

Office 365 Management Activity

Fournit des informations sur les actions et les événements des utilisateurs, administrateurs, systèmes et politiques de sécurité à partir des journaux Office 365 et Azure Active Directory.

Sophos Cloud

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

Produit vendu séparément ; intégré sans frais supplémentaires.

Conservation des données pendant 90 jours

Conserve les données de tous les produits Sophos et de tous les produits tiers (non Sophos) dans le Sophos Data Lake.

Protection Endpoint tierce

Compatible avec...

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

Intégrations complémentaires

Les données de sécurité provenant des sources tierces suivantes peuvent être intégrées pour être utilisées par l'équipe Sophos MDR via l'achat de 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, mener des chasses aux menaces et activer des capacités de réponse supplémentaires.

Sophos Network Detection and Response

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...

- Palo Alto Networks
- Fortinet
- Check Point
- Cisco
- SonicWall

Identité

Compatible avec...

- Okta
- Duo
- ManageEngine

Cloud public

Compatible avec...

- AWS Security Hub
- AWS CloudTrail
- Orca Security
- Google Cloud Platform Security

Messagerie

Compatible avec...

- Proofpoint
- Mimecast

Réseau

Compatible avec...

- Darktrace
- Tinkst Canary
- Skyhigh Security

Conservation des données pendant 1 an

Service Sophos MDR Guided Onboarding

Vous pouvez acheter en supplément l'option Sophos MDR Guided Onboarding pour une assistance à distance. Ce service fournit une assistance personnelle pour un déploiement efficace et en douceur, garantit des configurations conformes aux bonnes pratiques de sécurité et dispense une formation afin de maximiser la valeur de votre investissement dans le service MDR. Vous bénéficierez d'un interlocuteur dédié au sein des Services professionnels de Sophos qui vous accompagnera pendant les 90 premiers jours pour assurer la réussite de votre implémentation. Sophos MDR Guided Onboarding inclut :

Jour 1 – Implémentation

- Démarrage du projet
- Configuration de Sophos Central et revue des fonctionnalités
- Construction et test du processus de déploiement
- Configuration des intégrations MDR
- Configuration du ou des capteurs Sophos NDR
- Déploiement à l'échelle de l'entreprise

Jour 30 – Formation au XDR

- Formation pour penser et agir comme un SOC
- Formation pour rechercher les indicateurs de compromission
- Formation pour utiliser notre plateforme XDR pour les tâches admin
- Formation pour créer des requêtes pour des investigations futures

Jour 90 – Évaluation de la posture de sécurité

- Examen des politiques actuelles afin de proposer des recommandations conformes aux bonnes pratiques de sécurité
- Discussion autour des fonctionnalités inutilisées qui pourraient fournir une protection supplémentaire
- Évaluation de la sécurité selon le cadre NIST
- Réception d'un rapport de synthèse contenant les recommandations issues de notre évaluation

Pour en savoir plus :

sophos.fr/mdr

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

© Copyright 2023. Sophos Ltd. Tous droits réservés.
Immatriculée en Angleterre et au Pays de Galles N° 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.

23-01-24 DS-FR (DD)

SOPHOS