

# Sophos Managed Detection and Response



## Détection et réponse aux menaces 24/7

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 MDR (Managed 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 seuls  
Nos outils bloquent automatiquement 99,98 % des menaces. Nos analystes peuvent ainsi se concentrer pleinement 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 organisation. 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.

## Un service MDR qui s'adapte à vous

Sophos MDR est personnalisable avec plusieurs 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 24/7

Nous détectons et répondons aux menaces avant qu'elles ne puissent compromettre vos données ou entraîner des temps d'arrêt. Soutenu par 7 centres d'opérations de sécurité (SOC) dans le monde, Sophos MDR offre une couverture 24 h/24.

#### Compatible avec les outils de sécurité non Sophos

Sophos MDR peut intégrer la télémétrie provenant de technologies tierces : solutions endpoint, pare-feu, réseau, gestion d'identité, messagerie, sauvegarde et récupération, et bien d'autres encore.

#### 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. Avec une licence Sophos MDR Complete, vous bénéficiez de la réponse aux incidents complète et illimitée, sans plafond ni frais supplémentaires.

#### 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 menée 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 24/7/365, 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.

#### Intégrité du compte Sophos

Nous examinons en continu les paramètres et les configurations des systèmes endpoints gérés par Sophos MDR 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.

## 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, chasser les menaces, et activer des capacités de réponse supplémentaires.

### **Sophos Endpoint**

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

Produit inclus dans le prix de Sophos MDR.

### **Workload Protection**

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

Produit inclus dans le prix de Sophos MDR.

### **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.

### **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 ; abonnement Xstream Protection requis ; intégré sans frais supplémentaires

### **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.

### **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.

### **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 Office 365
- Defender for Cloud Apps
- Defender for Identity
- Entra ID Protection
- Microsoft 365 Defender
- Microsoft Purview DLP

### **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.

### **Microsoft Office 365 Management Activity**

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**

Intègre 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 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, chasser les menaces, et activer des capacités de réponse supplémentaires.

 <b>Sophos NDR</b> <p>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.</p> <p>Compatible avec n'importe quel réseau via le miroir de port SPAN.</p>	 <b>Firewall</b> <p>Compatible avec :</p> <ul style="list-style-type: none"><li>• Barracuda</li><li>• Check Point</li><li>• Cisco Firepower</li><li>• Cisco Meraki</li><li>• Fortinet</li><li>• F5</li><li>• Forcepoint</li><li>• Palo Alto Networks</li><li>• SonicWall</li><li>• WatchGuard</li></ul>	 <b>Réseau</b> <p>Compatible avec :</p> <ul style="list-style-type: none"><li>• Cisco Umbrella</li><li>• Darktrace</li><li>• Secutec</li><li>• Skyhigh Security</li><li>• Thinkst Canary</li><li>• Vectra</li><li>• Zscaler</li></ul>
 <b>Gestion d'identité</b> <p>Compatible avec :</p> <ul style="list-style-type: none"><li>• Auth0</li><li>• Cisco ISE</li><li>• Duo</li><li>• ManageEngine</li><li>• Okta</li></ul> <p>Intégration Microsoft incluse sans frais supplémentaires</p>	 <b>Messagerie</b> <p>Compatible avec :</p> <ul style="list-style-type: none"><li>• Mimecast</li><li>• Proofpoint</li></ul> <p>Intégrations Microsoft 365 et Google Workspace incluses sans frais supplémentaires.</p>	 <b>Cloud</b> <p>Compatible avec :</p> <ul style="list-style-type: none"><li>• Orca Security</li></ul> <p>Intégrations AWS, Azure et GCP incluses avec le produit Sophos Cloud, vendu séparément.</p>
 <b>Sauvegarde et restauration</b> <p>Compatible avec :</p> <ul style="list-style-type: none"><li>• Acronis</li><li>• Veeam</li></ul>	 <b>Conservation des données pendant 1 an</b> <p>Conserve les données des produits Sophos et des solutions tierces (non Sophos) dans le Sophos Data Lake.</p>	

## Service complémentaire

 <b>Sophos Managed Risk, optimisé par Tenable</b> <p>Réduisez vos cyber risques avec un service proactif de gestion des vulnérabilités de la surface d'attaque, fourni en tant que service.</p> <p>Sophos Managed Risk identifie les vulnérabilités de haute priorité pour vous permettre d'agir et de prévenir les attaques avant qu'elles ne perturbent votre activité. Disponible en tant que module complémentaire pour Sophos MDR.</p>
---

## Niveaux de service de Sophos

	Sophos MDR Essentials	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 »	✓	✓
Intégrité du compte Sophos	✓	✓
Chasse aux menaces dirigée par des experts	✓	✓
Confinement des menaces : les attaques sont interceptées, bloquant leur propagation Utilise l'agent complet Sophos MDR (protection, détection et réponse) ou Sophos MDR 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 MDR (protection, détection et réponse)	Contrat IR complémentaire	✓
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		✓

## Service Sophos MDR Guided Onboarding

Disponible en tant qu'achat supplémentaire optionnel, le service Sophos MDR Guided Onboarding vous offre une assistance à distance pour l'onboarding. 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 MDR

- Formation pour penser et agir comme un SOC
- Formation pour rechercher les indicateurs de compromission
- Formation pour utiliser notre plateforme MDR 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

## Découvrez pourquoi les clients choisissent Sophos MDR

Sophos est un leader établi en matière de détection et de réponse aux menaces, avec de multiples reconnaissances de l'industrie à l'appui.



Leader dans l'édition 2024 de l'IDC MarketScape dans la catégorie 'Worldwide Managed Detection and Response Services'



Nommé Gartner Peer Insights Customers' Choice dans la catégorie MDR (Managed Detection and Response).



Classé Leader par les clients dans le rapport G2 Grid® Summer 2024 dans la catégorie 'Managed Detection and Response'



Un Leader dans l'édition 2024 du rapport Global Managed Detection and Response de Frost Radar



Reconnu comme Strong Performer dans les évaluations MITRE Engenuity ATT&CK pour les services MDR

Pour en savoir plus :

[sophos.fr/mdr](https://sophos.fr/mdr)

Sophos France  
Tél. : 01 34 34 80 00  
Email : [info@sophos.fr](mailto:info@sophos.fr)

© Copyright 2024. 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.

2024-07-18 BRFR (PS)

**SOPHOS**