SOPHOS

Renforcer Microsoft Defender avec Sophos MDR

Réduisez vos cyber-risques, décuplez l'efficacité et l'impact de vos investissements de sécurité, et améliorez votre assurabilité en renforçant Microsoft Defender avec le service de détection et de réponse assuré 24/7 par le fournisseur de services MDR le plus fiable sur le marché.

Un livre blanc Sophos. Juillet 2023

Introduction

Une protection Endpoint est une couche de protection essentielle, mais elle ne suffit pas à bloquer toutes les menaces. Les cybercriminels sophistiqués d'aujourd'hui n'ont de cesse de perfectionner leurs tactiques, techniques et procédures d'attaque (TTP) pour échapper aux technologies de sécurité, en exploitant des vulnérabilités non corrigées, en volant des identifiants ou en abusant d'outils IT légitimes.

Pour bloquer les violations de sécurité et les attaques de ransomware actuelles, il est indispensable de renforcer Microsoft Defender à l'aide d'une équipe d'experts en détection et en réponse, disponible 24 h/24 et 7 j/7. En effet, face au volume d'alertes généré par les technologies Microsoft et à la complexité du paysage des menaces, les opérations de sécurité deviennent une tâche colossale, ardue et chronophage pour la plupart des entreprises.

C'est ce qui explique qu'un nombre croissant d'entre elles font appel à Sophos, le fournisseur de services MDR (Managed Detection and Response) le plus fiable et le mieux noté sur le marché, pour renforcer leur produit Microsoft Defender. Les analystes de Sophos surveillent, priorisent et répondent aux alertes de la Sécurité Microsoft 24 h/24 et 7 j/7, en intervenant immédiatement pour stopper les menaces confirmées. Ils utilisent également les technologies propriétaires de Sophos : détection, renseignements sur les menaces et chasse aux menaces pilotées par des experts, pour détecter et bloquer les menaces au-delà de Microsoft Defender.

Sophos MDR est conçu pour s'adapter à vous, en travaillant avec vos ressources internes et vos investissements informatiques et de sécurité existants. Quels que soient vos besoins : complémenter votre équipe interne avec une expertise additionnelle, étendre vos cyberdéfenses avec une couverture en dehors des heures de travail, ou externaliser entièrement le travail de détection et de réponse aux menaces, Sophos MDR vous aide à obtenir de meilleurs résultats en matière de cybersécurité.

Renforcer Microsoft Defender avec Sophos MDR

✓ Réduisez vos cyber-risques

- Bloquez les violations de sécurité et les attaques de ransomware avancées, y compris les menaces orchestrées manuellement capables de contourner Microsoft Defender

✓ Décuplez l'efficacité et l'impact de vos investissements de sécurité

- Libérez vos ressources informatiques pour mieux vous consacrer à vos projets stratégiques
- Réduisez la probabilité d'encourir des coûts de rétablissement associés à un incident majeur
- Obtenez un meilleur retour sur vos investissements existants

✓ Améliorez votre assurabilité

- Bénéficiez de meilleures offres d'assurance, qui prennent en compte et récompensent vos efforts déployés pour réduire vos cyber-risques

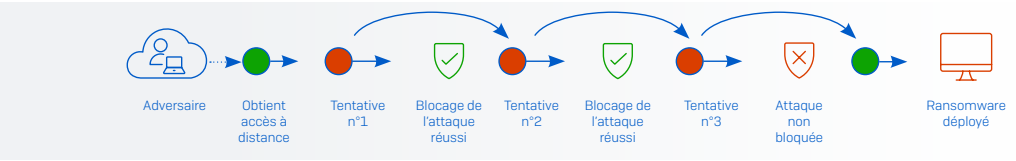
Les attaquants n'entrent pas par effraction – Ils se connectent

Dans la réalité, les solutions technologiques à elles seules, y compris Microsoft Defender, ne peuvent empêcher toutes les cyberattaques. Les adversaires actifs sont des attaquants qui adaptent leurs tactiques, techniques et procédures (TTP) sur le vif, agissant en temps réel sur leur clavier en réponse aux actions des défenseurs et de leurs outils de sécurité, mais aussi pour échapper à la détection.

Ces attaques, qui se traduisent souvent par des incidents impliquant des ransomwares dévastateurs et des violations de données, sont parmi les plus difficiles à stopper. Et elles se généralisent : 23 % des petites et moyennes entreprises rapportent avoir subi une attaque impliquant un adversaire actif au cours des douze derniers mois. Reflétant le potentiel dévastateur de ces attaques, 30 % des responsables IT/sécurité considèrent les adversaires actifs comme l'une de leurs principales préoccupations en 2023.[1].

Mais pour les contrecarrer, il ne suffit pas de les bloquer avec des technologies de sécurité. Ces acteurs malveillants, persistants et chevronnés, déploient une multitude d'approches toujours plus innovantes pour atteindre leurs objectifs, notamment :

- Exploiter les failles de sécurité pour pénétrer le réseau de l'entreprise et se déplacer latéralement une fois à l'intérieur, à l'aide d'identifiants volés, de failles non corrigées ou d'erreurs de configuration des outils de sécurité.
- Abuser les outils IT légitimes utilisés par les défenseurs pour éviter de déclencher des détections, notamment PowerShell, PsExec et le RDP.



Exemple de stratégie d'attaque d'un adversaire actif

- Modifier leurs attaques en temps réel en réponse aux contrôles de sécurité, en continuant d'utiliser de nouvelles techniques jusqu'à ce qu'ils trouvent le moyen d'atteindre leurs objectifs.

En se faisant passer pour des utilisateurs autorisés et en tirant profit des failles dans les défenses des entreprises, les acteurs malveillants parviennent à éviter de déclencher les technologies de détection automatique qui peinent à distinguer les attaquants des utilisateurs légitimes.

Et la tâche devient de plus en plus ardue pour les défenseurs face à des adversaires qui, aujourd'hui, disposent de moyens financiers pour innover sans relâche et parfaire leur business model. La progression accélérée du modèle de cybercrime en tant que service, et notamment du « ransomware-as-a-service » et du « phishing-as-a-service », rend le terrain de jeu de plus en plus accessible pour les cybercriminels en herbe qui souhaitent se lancer, tout en facilitant une exécution à grande échelle et en améliorant la qualité des attaques.

Conséquence de cette évolution des cybermenaces, le taux de chiffrement des données à cause d'un ransomware n'a jamais été aussi élevé — les cybercriminels parvenant à chiffrer les données dans plus de trois quarts (76 %) des attaques[2].

La réalité des ransomwares

- 66 % des entreprises déclarent avoir été touchées par un ransomware au cours de l'année passée.
- Dans 76 % des attaques de ransomware, les données ont été chiffrées.
- Dans 30 % des attaques où des données ont été chiffrées, les données ont également été volées.
- 1er vecteur d'attaque : vulnérabilité exploitée (36 %)
- 2e vecteur d'attaque : compromission d'identifiants (29 %)

1 L'état de la cybersécurité en 2023 : l'impact des cyberattaques sur les entreprises, Sophos

2 L'état des ransomwares 2023, Sophos.

Détection et réponse aux menaces 24/7 : une composante essentielle de la cyber-sécurité moderne

La bonne nouvelle, c'est qu'en associant technologie et expertise humaine, il est possible de stopper les attaques avancées pilotées par les attaquants. À chaque fois qu'un adversaire agit, un signal est créé. En combinant l'expertise humaine avec des modèles avancés de Machine Learning basés sur l'IA et des outils XDR (Extended Detection and Response), les spécialistes peuvent exploiter les signaux des technologies IT/sécurité pour détecter, investiguer et neutraliser les attaques, même les plus avancées, empêchant ainsi les ransomwares et les vols de données.

Alors que la détection et la réponse aux menaces 24/7 constituent désormais un élément essentiel de tout dispositif de cybersécurité, la plupart des entreprises ont du mal à les mettre en œuvre de manière efficace, ce qui les expose aux attaques. Les deux obstacles les plus courants sont le manque d'expertise et le manque de personnel qualifié.

Défi numéro 1 : le manque d'expertise

Détecter, investiguer et répondre aux menaces est un travail de haut niveau qui nécessite une connaissance approfondie des techniques d'attaque et des stratégies d'investigation, ainsi qu'une excellente maîtrise des outils utilisés par les défenseurs. Peu d'entreprises disposent en interne de cet ensemble de compétences complexes (et coûteuses), et en réalité, 93 % d'entre elles admettent que l'exécution des tâches essentielles liées aux opérations de sécurité est un réel défi :

- 71 % des entreprises ont du mal à identifier les signaux du bruit de fond (c'est-à-dire comprendre quels signaux/alertes doivent être examinés)
- 71 % des entreprises ont du mal à obtenir suffisamment d'informations pour déterminer si un signal est malveillant ou bénin
- 75 % des entreprises ont du mal à identifier la cause première de l'incident (c'est-à-dire la manière dont l'adversaire s'est introduit dans l'entreprise)

La difficulté de la tâche est on ne peut plus claire si l'on examine les données que les défenseurs reçoivent en provenance de leurs outils de sécurité. Ce tableau contient une liste non exhaustive des événements Microsoft Defender, ainsi que leur classification.

Comprendre l'alerte ne représente qu'une partie du processus. Les défenseurs doivent ensuite appliquer des informations contextuelles et corréler le tout avec des renseignements sur les menaces pour pouvoir parfaitement appréhender la menace et identifier le meilleur plan d'action.

TITRE DE L'ÉVÉNEMENT	TYPE D'ÉVÉNEMENT
Clic sur URL suspecte	Accès initial
Connexions réseau ou fichiers malveillants associés au processus 3CXDesktopApp.exe	Malware
Nouveau compte utilisateur créé	Persistance
TS_BL_Suspicious Eventlog Clear ou Configuration utilisant Wevtutil	Contournement des défenses
Élévation des privilèges des processus	Élévation des privilèges
Tentative de désactivation de la protection antivirus Microsoft Defender	Contournement des défenses
Fichier ou connexion réseau liée à l'acteur malveillant Storm-0867 détectée	Accès aux identifiants
Moteurs TS_BL_Script se connectant à Internet	Command and Control
Activité malveillante potentielle opérée manuellement	Activité suspecte
Téléchargement de charges utiles malveillantes TS_BL_ via binaires Office	Exécution
Groupe de menaces émergent DEV-0867 détecté	Accès aux identifiants
Groupe de menaces émergent Citrine Sleet détecté	Malware

Exemple de cas de détection issus de Microsoft Defender

Défi numéro 2 : le manque de personnel qualifié

Détecter, investiguer et répondre aux menaces constitue un travail chronophage. À titre d'exemple, le temps moyen de traitement d'une alerte de sécurité (détection, investigation et réponse) est de 9 heures pour les entreprises de 100 à 3 000 employés et de 15 heures pour celles de 3 001 à 5 000 employés.

Cette tâche représente donc un nombre considérable d'heures prises sur le travail des équipes informatiques, d'autant plus que la nature urgente de certains événements peut les empêcher de concentrer leurs efforts sur des défis plus stratégiques. De plus, les adversaires exécutant des attaques à toute heure du jour ou de la nuit, le travail de détection et de réponse aux menaces doit s'effectuer 24 h/24, 7 j/7 et 365 j/an pour un impact maximal. Or, bon nombre d'entreprises, pour ne pas dire la plupart d'entre elles, n'ont pas les ressources nécessaires.

Solution : compléter les défenses avec un service managé de détection et de réponse (MDR)

Aujourd'hui, 52 % des responsables IT/cybersécurité admettent que les cybermenaces sont désormais trop avancées pour que leur entreprise puisse y faire face seule. C'est pourquoi ils se tournent de plus en plus vers des fournisseurs spécialisés dans les services MDR, tels que Sophos, pour compléter et étendre leurs capacités en interne.

Définition du MDR

Un service MDR (Managed Detection and Response) est un service entièrement managé pour vous, 24 h/24 et 7 j/7, assuré par des experts spécialisés dans la détection et la réponse aux cyberattaques, que les solutions technologiques seules ne peuvent empêcher.

La technologie XDR (Extended Detection and Response) est une plateforme qui unifie les données de sécurité provenant de sources multiples afin d'automatiser et d'accélérer la détection, l'investigation et la réponse aux menaces, ce que les solutions de sécurités individuelles isolées ne peuvent pas faire.

Les spécialistes MDR de Sophos s'appuient sur la plateforme Sophos XDR pour chasser, investiguer et neutraliser les menaces pour vous. Ils exploitent les signaux provenant de l'ensemble de l'infrastructure informatique, dont le pare-feu, la messagerie, le Cloud et les mobiles, afin d'accélérer la détection et la réponse aux menaces.

Renforcer Microsoft Defender avec Sophos MDR

Sophos MDR fournit un service de détection et de réponse aux menaces 24/7 pour les environnements Microsoft Defender. Les analystes de Sophos surveillent, priorisent et répondent aux alertes de la Sécurité Microsoft 24 h/24 et 7 j/7, en intervenant immédiatement pour stopper les menaces confirmées. Ils utilisent également les technologies propriétaires de Sophos : détection, renseignements sur les menaces et chasse aux menaces pilotées par des experts, pour détecter et bloquer les menaces au-delà de Microsoft Defender.

Plus notre visibilité sera large, plus vite nous pourrons agir. Sophos MDR exploite d'autres sources d'événements de la Sécurité Microsoft qui sont incluses dans les licences E3 et E5, ainsi que les signaux provenant des solutions déjà en place — pare-feu, cloud, messagerie, gestion d'identité et NDR (Network Detection and Response) — pour accélérer la détection et la réponse aux menaces.

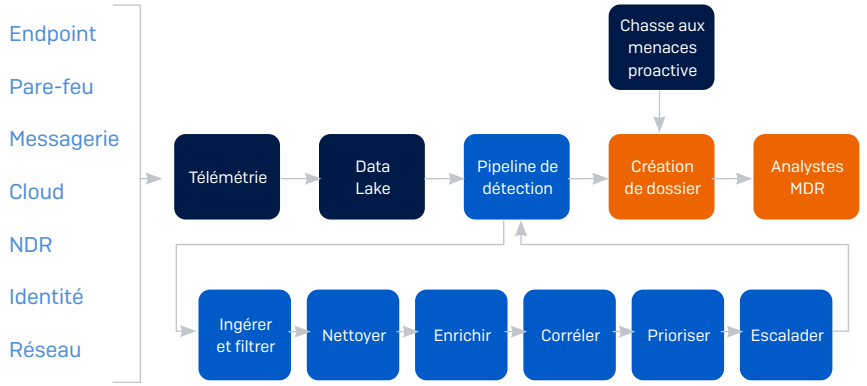
Les utilisateurs de Microsoft Defender bénéficient d'un accès immédiat aux experts en sécurité de Sophos par téléphone 24 h/24 et 7 j/7, mais aussi de rapports détaillés sur l'activité des menaces dans la plateforme Sophos Central.

Sophos MDR pour Microsoft Defender est compatible avec les sources d'événements de la Sécurité Microsoft

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- Centre de sécurité et de conformité MS 0365
- Microsoft Azure Sentinel
- Activité de gestion Office 365 (journal d'audit unifié)

Le 'Security Event Flow' de Sophos MDR

Notre Security Event Flow (flux des événements de sécurité) breveté est un élément clé du service Sophos MDR. La télémétrie provenant de l'ensemble de l'environnement de sécurité, y compris de Microsoft Defender, est ingérée par le Data Lake de Sophos, puis traitée via notre pipeline de détection, qui convertit l'énorme volume d'alertes de Microsoft et de solutions tierces en informations utilisables et priorisées qui nous permettent d'investiguer et de répondre efficacement.



Le Security Event Flow de Sophos MDR

Ingérer et filtrer – Ingère la télémétrie et filtre les bruits indésirables

Nettoyer – Transforme les données en schéma normalisé et les corrèle avec MITRE ATT&CK®.

Enrichir – Ajouter des renseignements supplémentaires sur les menaces provenant de tiers et des informations contextuelles sur l'entreprise

Corréler – Regroupe les alertes en fonction des entités, de la classification MITRE ATT&CK et de l'heure.

Prioriser – Classe les alertes et les regroupe par ordre de priorité

Escalader – Applique une logique pour escalader les clusters en dossiers à investiguer.

Couverture 24/7 assurée par sept centres d'opérations de sécurité (SOC) à travers le monde

Les menaces sont examinées et remédiées par une équipe mondiale d'experts en détection et en réponse aux menaces, basée dans sept centres d'opérations de sécurité (SOC) répartis en Amérique du Nord (Indiana, Utah, Hawaï), en Europe (Royaume-Uni/Irlande, Allemagne) et dans la région Asie-Pacifique (Inde, Australie). Avec plus de 500 experts couvrant l'ensemble de l'environnement des menaces (malwares, automatisation, IA et remédiation), Sophos MDR dispose d'une étendue et d'une profondeur d'expertise qu'il est quasiment impossible de répliquer en interne.

Leader mondial en matière de temps de détection et de réponse

Cette approche unique qui combine expertise humaine, technologie et renseignements sur les menaces permet à Sophos MDR de garantir un temps de réponse aux incidents de 38 minutes seulement en moyenne. Ce record mondial, à son tour, permet l'obtention de meilleurs résultats de cybersécurité :

- Temps moyen de détection (MTTD) : 1 minute
- Temps moyen d'investigation (MTTI) : 25 minutes
- Temps moyen de réponse (MTTR) : 12 minutes

Qui utilise Sophos MDR ?

Des milliers d'entreprises issues de tous les secteurs utilisent le service Sophos MDR, aussi bien des petites entreprises disposant de ressources informatiques limitées que de grandes entreprises dotées d'un SOC interne. Les trois modèles de réponse Sophos MDR les plus populaires sont les suivants :

- Sophos MDR gère entièrement la réponse aux menaces à la place du client
- Sophos MDR collabore avec l'équipe interne, en gérant conjointement la réponse aux menaces
- Sophos MDR apporte son aide à l'équipe interne, en l'alertant sur les incidents qui requièrent une action et en lui fournissant des informations sur les menaces et des conseils de remédiation.

Exemple de scénario : utiliser Microsoft Defender pour détecter le Command-and-Control

SECTEUR
Services professionnels

SIÈGE
États-Unis

EFFECTIF
750 employés

NIVEAU DE SERVICE
Sophos MDR pour Microsoft Defender

SOURCES DE TÉLÉMÉTRIE INTÉGRÉES À SOPHOS MDR

✓ Endpoint	X Identité
✓ Pare-feu	X Cloud
X Messagerie	✓ Réseau

Qu'est-ce que le « Command-and-Control » ?

Le « Command-and-Control » (également appelé C&C ou C2) englobe des techniques utilisées par les attaquants pour communiquer avec les systèmes qu'ils contrôlent au sein du réseau de leur victime et leur envoyer des commandes.

Les canaux C&C entre l'environnement cible et l'infrastructure de l'attaquant peuvent être établis de diverses manières, par exemple par le biais d'emails de phishing, de l'ingénierie sociale, d'un malware, de failles dans les plugins de navigateur, etc. Souvent, les adversaires utilisent les ressources communément disponibles et imitent le trafic réseau attendu pour éviter d'être suspectés et détectés.

DÉTECTION

Microsoft Defender génère une alerte en cas de communication avec une adresse IP malveillante.

L'alerte Microsoft est automatiquement mise en corrélation avec les événements du Data Lake de Sophos XDR afin de déterminer si l'attaque a été bloquée par le pare-feu du client et si elle affecte plusieurs postes de travail.

INVESTIGATION

Les analystes de Sophos MDR confirment que la connexion malveillante signalée par l'alerte Microsoft Defender a été bloquée et que la menace immédiate est contenue.

SophosLabs Intelix est utilisé pour identifier la famille de l'attaque, les indicateurs de compromission (IOC), ainsi que les IP et domaines connus utilisés par l'attaquant.

L'alerte Microsoft de départ est enrichie de ces renseignements sur les menaces pour permettre une analyse détaillée de l'attaque (RCA).

RÉPONSE

L'appareil compromis est isolé et l'attaque est contenue.

Sophos MDR confirme que l'accès initial a été obtenu par un email de phishing. Une investigation est menée pour identifier la composition de l'email de phishing et s'assurer qu'aucun autre compte utilisateur n'est compromis.

Sophos fournit des recommandations pour réduire la probabilité de réussite des attaques de phishing à l'avenir.

Avantages clients

Quel que soit votre besoin : complémenter votre équipe interne dédiée aux opérations de sécurité ou bénéficier d'un service 24/7 de détection et de réponse, assuré par des experts, sans avoir à assumer la charge opérationnelle liée à la mise en place votre propre SOC, Sophos MDR peut vous aider. Les entreprises qui choisissent de renforcer Microsoft Defender avec Sophos MDR obtiennent de meilleurs résultats : un cyber-risque réduit, un meilleur retour sur leurs investissements de sécurité (plus efficaces et plus mesurables) et une meilleure assurabilité.

Bloquer les menaces avancées avec Microsoft + Sophos MDR

Surveillance et réponse 24/7 assurées par une équipe d'experts
Les analystes de Sophos MDR surveillent, priorisent et répondent aux alertes de sécurité Microsoft Defender 24 h/24 et 7 j/7, en intervenant immédiatement pour stopper les menaces confirmées.

Détecter et bloquer les menaces qui contournent la protection Microsoft Defender
Les détections propriétaires de Sophos, ainsi que les renseignements sur les menaces et les chasses aux menaces assurées par des experts ajoutent des couches de défense supplémentaires.

Améliorer la visibilité et contextualiser les alertes Microsoft Defender
Intégrez d'autres sources d'événements de la Sécurité Microsoft qui sont incluses dans votre licence E3 ou E5

Accès immédiat à des spécialistes en opérations de sécurité
Les analystes de Sophos MDR sont accessibles par téléphone 24 h/24 et 7 j/7, et des rapports détaillés sur l'activité des menaces sont disponibles dans Sophos Central.

Réduire le cyber-risque

L'un des principaux avantages du renforcement de Microsoft Defender par Sophos MDR est l'obtention d'une protection accrue contre les ransomwares et toute autre menace avancée.

Les analystes de Sophos bénéficient d'une expérience inégalée, mais aussi d'une maîtrise des outils de télémétrie et de chasse aux menaces qui est pratiquement impossible de reproduire en interne. Cette expertise leur permet de répondre plus rapidement et plus précisément à toutes les étapes du processus, de l'identification des signaux importants à l'investigation des incidents potentiels et à la neutralisation des activités malveillantes.

Avec Sophos MDR, Sophos sécurise plus d'entreprises que n'importe quel autre fournisseur, ce qui nous permet de fournir une « immunité communautaire » sans précédent. Les informations tirées de la défense d'un client sont automatiquement appliquées à tous les autres clients ayant un profil similaire, ce qui nous permet de prévenir de manière proactive des attaques similaires dans cette communauté.

★★★★★

« Les pen-testeurs ont été choqués de ne pas pouvoir trouver un moyen d'entrer. C'est à ce moment-là que nous avons su que nous pouvions absolument faire confiance au service de Sophos ».

Université de South Queensland, Australie

★★★★★

« Avec Sophos MDR, nous avons réduit considérablement notre temps de réponse aux menaces. »

Tata BlueScope Steel, Inde

★★★★★

« Nous sommes informés de toute menace en temps réel. »

Bardiani Valvole, Italie

Décuplez l'efficacité et l'impact de vos investissements de sécurité

Sophos MDR vous permet d'accroître l'efficacité et l'impact de votre personnel et de vos outils de sécurité.

En effet, le travail de détection et de réponse aux menaces mobilise beaucoup de moyens IT. En prenant en charge cette tâche, Sophos MDR libère vos ressources informatiques qui pourront se consacrer pleinement à la mise en œuvre de vos projets stratégiques. Parallèlement, un accès téléphonique 24 h/24 et 7 j/7 aux experts en sécurité Sophos et des rapports détaillés sur l'activité des menaces depuis la plateforme Sophos Central, accélèrent le travail des équipes internes en leur permettant de répondre plus rapidement et avec plus de précision aux alertes.

En utilisant la télémétrie de vos outils Microsoft et de vos outils tiers existants pour accélérer la détection et la réponse aux menaces, Sophos MDR élève vos défenses tout en vous permettant d'accroître votre retour sur investissement.

En outre, avec une facture moyenne de 1,85 million de dollars pour remédier à une attaque de ransomware et 84 % des victimes de ransomware déclarant que l'attaque leur a fait perdre de l'activité/du chiffre d'affaires[2], l'investissement dans un service tel que Sophos MDR réduit le coût total de possession de la cybersécurité.

★★★★★

« Depuis l'implémentation de Sophos, nous avons réussi à libérer des heures opérationnelles importantes qui ont permis à nos équipes de se concentrer sur des initiatives qui ont augmenté la satisfaction de nos étudiants. »

London South Bank University, Royaume-Uni

★★★★★

« La capacité de Sophos MDR à traiter les menaces ou à les supprimer rapidement et à les porter à notre connaissance nous libère pour nous concentrer sur des tâches à forte valeur ajoutée ».

Tomago Aluminium, Australie

Améliorez votre assurabilité

Sophos MDR permet aux entreprises de se doter des nombreux contrôles essentiels pour être assurable et bénéficier de meilleures polices d'assurance : détection et réponse 24/7, planification de la réponse aux cyber incidents, journalisation et surveillance, etc.

Les clients font état d'un meilleur accès à une couverture d'assurance, ainsi que de polices qui reconnaissent et récompensent leurs efforts déployés pour réduire leurs cyber-risques.

★★★★★

« Notre décision de nous allier à Sophos pour le XDR et le MDR a été un facteur déterminant dans la diminution de nos primes de cybersécurité par rapport à ce qu'on nous avait annoncé au départ, à savoir des primes multipliées par deux. C'est un pari gagnant que nous avons fait, qui nous a procuré une réelle valeur ajoutée… J'ai même reçu un mot du directeur financier remerciant mon équipe pour les économies réalisées, et c'est grâce au MDR. »

Bob Pellerin, CISO, The Fresh Market, États-Unis

2 L'état des ransomwares 2023, Sophos

Le service MDR le plus fiable sur le marché

Sophos est le premier fournisseur MDR sur le marché, sécurisant plus d'entreprises que tout autre éditeur, contre les ransomwares, violations et autres menaces que la technologie seule ne peut pas stopper.

Sophos MDR protège des milliers d'entreprises de tous secteurs industriels à travers le monde, ce qui nous permet d'avoir une expertise inégalée sur les menaces qui pèsent sur chacun de ces secteurs. Nous tirons parti de cette télémétrie étendue pour générer une « immunité communautaire », en appliquant les enseignements tirés de la défense d'une entreprise à tous les autres clients au profil similaire, nous permettant ainsi d'élever les défenses de chacun.

Bien entendu, ce qui compte le plus, ce sont les résultats de cybersécurité que nous obtenons pour nos clients. Sophos est la solution MDR la mieux notée et la plus évaluée sur Gartner® Peer Insights™ avec une note de 4,8/5 sur 300 avis au 14 juin 2023, avec 97 % des clients déclarant qu'ils nous recommanderaient.

Sophos est également nommé Leader dans les rapports G2 Grid® pour les services MDR, ainsi que Leader dans la catégorie MDR dans les segments G2 Overall, Midmarket et Enterprise.

Pour en savoir plus sur Sophos MDR et sur la façon dont le service permet aux utilisateurs de Microsoft Defender de réduire leurs cyber-risques, de décupler l'efficacité et l'impact de leurs investissements de sécurité et d'améliorer leur assurabilité, consultez la page www.sophos.fr/mdr.

Le plus fiable

Plus de 17 000 entreprises utilisent Sophos MDR (T2, 2023)

Le mieux noté

Note des clients de 4,8 sur 5

Le plus évalué

300 avis sur Gartner Peer Insights sur les 12 derniers mois

Découvrez la protection Sophos Endpoint

La protection Sophos Intercept X Endpoint travaille pour vous et avec vous, en adaptant vos défenses en fonction de l'attaque.

Puissante et multicouche, elle offre une protection supérieure contre les ransomwares et les menaces avancées à tous les stades de la chaîne d'attaque, y compris la protection anti-ransomware basée sur le comportement et 60 mesures de prévention des exploits activées par défaut (aucun paramétrage requis).

Notre protection adaptative contre les attaques (Adaptive Attack Protection) innovante répond de manière dynamique aux attaques manuelles, en déployant automatiquement des défenses supplémentaires pour contrecarrer l'adversaire et donner aux défenseurs le temps de répondre.

Les utilisateurs du service Sophos MDR utilisant Microsoft Defender peuvent évoluer vers la protection Sophos Endpoint à tout moment, afin d'obtenir une flexibilité totale tout pérennisant leurs prochains déploiements de sécurité.

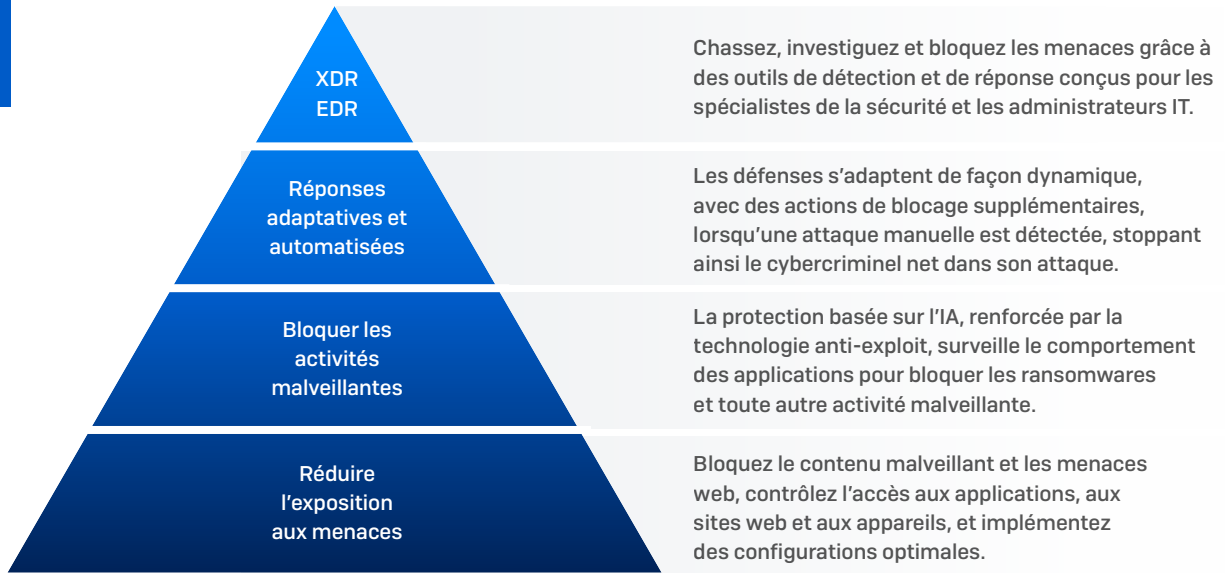
✓ Leader de Gartner 13 années consécutives
Sophos a été nommé Leader dans le Magic Quadrant de Gartner pour les solutions EPP depuis 2008.

✓ Le mieux noté sur Gartner Peer Insights
Note des clients de 4,8 sur 5.

✓ Leader de G2 pour les segments Enterprise, Midmarket et PME
Basé exclusivement sur les commentaires des clients.

✓ Score de protection de 100 % – SE Labs
Note AAA pour la sécurité des grandes entreprises et des PME.

Pour en savoir plus ou démarrer un essai gratuit : www.sophos.fr/endpoint



Gartner, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Chris Silva, 31 December 2022
GARTNER est une marque déposée et une marque de service de Gartner, Inc. et/ou de ses filiales aux États-Unis et dans le monde, Magic Quadrant et PEER INSIGHTS sont des marques déposées de Gartner, Inc. et/ou de ses filiales et sont utilisées ici avec autorisation. Tous droits réservés.
Gartner ne fait la promotion d'aucun fournisseur, produit ou service cité dans ses publications de recherche, et ne conseille aucunement aux utilisateurs de technologies de ne sélectionner que les fournisseurs ayant obtenu les meilleures notes ou toute autre distinction. Les publications de recherche de Gartner reflètent les opinions de l'organisme de recherche Gartner et ne devraient pas être interprétées comme un énoncé de faits. Gartner décline toute responsabilité, expresse ou implicite, liée à cette étude, y compris toute responsabilité quant à la valeur marchande ou à l'adéquation à un besoin particulier.
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.

Sophos fournit des solutions de cybersécurité de pointe aux entreprises de toutes tailles, les protégeant en temps réel contre les menaces avancées telles que les malwares, les ransomwares et le phishing. Grâce à des fonctionnalités Next-Gen éprouvées, les données de votre entreprise sont sécurisées efficacement par des produits alimentés par l'intelligence artificielle et le Machine Learning.

2023-06-27 (WP-NP)

SOPHOS