Brochure de la solution

Sophos Endpoint

Alimenté par Intercept X

La solution de sécurité Endpoint optimisée par l'IA la plus complète sur le marché

Optimisé par la technologie Intercept X, Sophos Endpoint offre une protection inégalée qui bloque les attaques sophistiquées avant qu'elles n'affectent vos systèmes. De puissants outils EDR/XDR (Endpoint/Extended Detection and Response) permettent à votre entreprise de chasser, d'investiguer et de répondre aux activités suspectes et aux indicateurs d'attaque.

Une approche de la sécurité axée sur la prévention

Sophos Endpoint ne s'appuie pas uniquement sur une seule technique de sécurité, mais adopte une approche globale axée sur la prévention pour protéger tous les postes de travail. De multiples modèles de Deep Learning IA protègent contre les attaques connues et inédites. Les contrôles du Web, des applications et des périphériques réduisent votre surface d'attaque et bloquent les vecteurs d'attaque courants. L'analyse comportementale, les technologies anti-ransomware et anti-exploit, ainsi que d'autres technologies de pointe bloquent rapidement les menaces avant qu'elles ne prennent de l'ampleur. Les équipes informatiques, dont les ressources sont limitées, ont ainsi moins d'incidents à investiguer et à résoudre.

Protection anti-ransomware imperméable

Sophos Endpoint est la protection endpoint zero-touch la plus robuste sur le marché contre les ransomwares sophistiqués. La technologie CryptoGuard bloque le chiffrement malveillant en temps réel et restaure automatiquement les fichiers affectés vers leur état d'origine sain, minimisant ainsi tout impact sur l'entreprise.

Défenses adaptatives

Les défenses dynamiques s'adaptent en réponse aux adversaires actifs et aux attaques pilotées manuellement. La capacité d'action de l'attaquant est neutralisée, vous faisant gagner un temps additionnel précieux pour lancer vos actions de réponse.

Facile à installer et à administrer

Sophos Central est une puissante plateforme Cloud de gestion de la cybersécurité qui unifie toutes les solutions de sécurité Next-Gen de Sophos. Les technologies et fonctionnalités recommandées sont activées par défaut, vous faisant bénéficier immédiatement de la protection la plus robuste, sans qu'aucun réglage ne soit nécessaire.

Un leader de confiance dans le domaine de la sécurité Endpoint

Sophos Endpoint est régulièrement salué par les clients, les analystes et les organismes de test indépendants. Sophos a été nommé 15 fois Leader dans le Gartner® Magic Quadrant™ pour les plateformes de protection Endpoint et a été classé n°1 des suites de protection Endpoint par G2 dans ses rapports Grid® Winter 2025.

Avantages principaux

- De multiples modèles de Deep Learning IA protègent contre les attaques connues et inédites.
- Réduisez votre surface d'attaque et bloquez les vecteurs courants grâce à des contrôles du Web, des applications et des périphériques.
- Bloquez rapidement les menaces avant qu'elles ne prennent de l'ampleur grâce à l'analyse comportementale, aux technologies anti-ransomware et anti-exploit, ainsi qu'à d'autres technologies de pointe.
- Protégez vos données contre les attaques de ransomwares locaux et distants grâce à une protection de premier ordre.
- Bénéficiez de défenses dynamiques inédites qui s'adaptent automatiquement en réponse à des adversaires actifs et à des attaques manuelles.
- Chassez, investiguez et répondez aux activités suspectes grâce à de puissants outils EDR et XDR.

Une approche axée sur la prévention réduit votre surface d'attaque

Il est moins coûteux de bloquer les attaques à un stade précoce de la chaîne d'attaque que de les surveiller et y remédier à un stade tardif. Sophos Endpoint inclut des technologies de protection sophistiquées qui bloquent les attaques les plus diverses. Les contrôles du Web, des applications et des périphériques réduisent votre surface d'attaque et bloquent les vecteurs d'attaque courants. Cela réduit ainsi les possibilités de pénétration des attaquants dans votre environnement.

Protection Web

Bloque le trafic sortant du navigateur vers les sites web malveillants pour stopper les menaces au stade de la diffusion et empêcher les sites de phishing ou de logiciels malveillants.

Contrôle du Web

Bloque l'accès aux contenus indésirables et inappropriés. Appliquez une politique d'utilisation acceptable du web au sein de votre entreprise et protégez-vous contre les fuites de données.

Réputation des téléchargements

Analyse les fichiers téléchargés à l'aide des renseignements sur les menaces fournis par les SophosLabs afin de fournir un verdict basé sur la prévalence, l'âge et la source. Les utilisateurs sont invités à bloquer les fichiers dont la réputation est faible ou inconnue.

Contrôle des applications

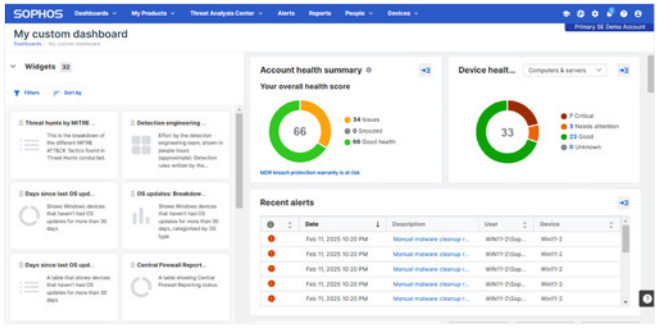
Bloque les applications vulnérables ou inadaptées à l'aide de catégories prédéfinies, ce qui évite de devoir bloquer chaque application individuellement selon leur hachage.

Contrôle des périphériques (appareils)

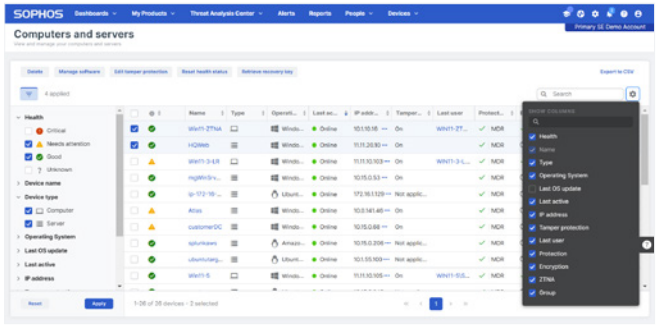
Surveille et bloque l'accès aux supports amovibles, au Bluetooth et aux appareils mobiles afin d'empêcher certains équipements de se connecter à votre réseau.

Prévention des pertes de données

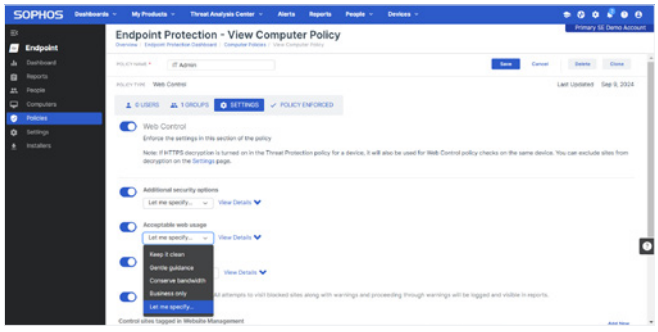
Surveillez ou limitez le transfert des fichiers contenant des données sensibles. Vous pouvez par exemple empêcher les utilisateurs d'envoyer un fichier confidentiel à l'aide d'une messagerie web.



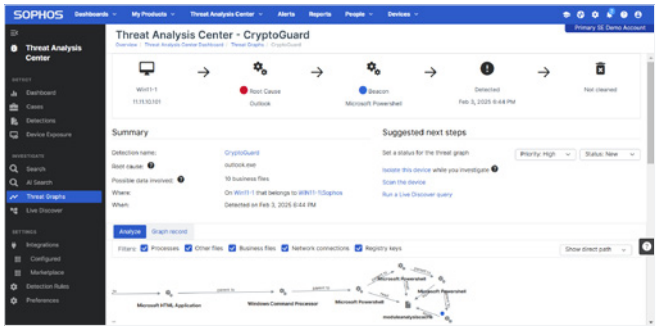
Création de tableaux de bord personnalisés pour répondre à vos besoins.



Sécurité Endpoint facile à configurer et à gérer.



Politiques configurables avec des paramètres recommandés activés par défaut.



Analyse des menaces pour en déterminer la cause première.

Une approche axée sur la prévention bloque rapidement les menaces

Réduisez les risques en détectant et en remédiant aux menaces le plus tôt possible. Sophos Endpoint bloque les menaces rapidement avant qu'elles ne s'aggravent, ce qui permet aux équipes informatiques, dont les ressources sont limitées, d'avoir moins d'incidents à investiguer et à résoudre. Sophos offre des capacités de prévention des menaces robustes, comme en attestent les notes exceptionnelles obtenues régulièrement dans les tests de sécurité indépendants.

Protection anti-ransomware imperméable

Selon le rapport '2024 Digital Defense' de Microsoft, le chiffrement à distance fait désormais partie de 70 % des attaques réussies, avec 92 % d'entre elles démarrant sur des appareils non gérés du réseau. Sophos Endpoint fournit la défense la plus puissante contre les ransomwares locaux et distants, en s'appuyant sur la technologie avancée CryptoGuard pour détecter les tentatives de chiffrement, quelle qu'en soit la source.

- Bloque les nouvelles variantes de ransomware.
- Inspecte les modifications de fichiers en temps réel afin de détecter tout chiffrement malveillant.
- Empêche les ransomwares de chiffrer les fichiers à distance sur le réseau.
- Restaure automatiquement tous les fichiers chiffrés vers leur état d'origine non chiffré, à l'aide d'une technologie exclusive qui ne repose pas sur le service VSS (Volume Shadow Copy Service) de Windows.
- Protège tous les types et toutes les tailles de fichiers avec un impact minimal sur les performances.
- Protège l'enregistrement de démarrage principal (MBR) contre les attaques avancées ciblant le disque dur.

Prévention des malwares basée sur le Deep Learning de l'IA

Détecte et bloque les malwares connus et inconnus en analysant les attributs des fichiers et en utilisant le raisonnement prédictif pour identifier les menaces.

Anti-exploit

Protège l'intégrité des processus grâce au durcissement de la mémoire et à plus de 60 techniques anti-exploit qui ne nécessitent aucun réglage et surpassent les capacités natives de Windows et d'autres solutions de sécurité.

Détection comportementale

Surveille les événements liés aux processus, aux fichiers et au registre afin de détecter et de bloquer les activités malveillantes. Elle analyse la mémoire, inspecte les processus en cours d'exécution à la recherche de menaces cachées et détecte les attaquants qui injectent du code malveillant pour échapper à la détection.

Sécurité Synchronisée

Sophos Endpoint partage les informations de sécurité avec Sophos Firewall, Sophos Zero Trust Network Access (ZTNA) et d'autres produits Sophos pour fournir une visibilité accrue sur les menaces et l'utilisation des applications, et isoler automatiquement les appareils compromis.

Live Protection

Étend la protection robuste sur l'appareil en accédant en temps réel aux renseignements sur les menaces des SophosLabs. Cela permet d'obtenir un contexte de fichier supplémentaire, de vérifier les décisions, de supprimer les faux positifs et d'analyser la réputation des fichiers.

Verrouillage des applications

Empêche l'utilisation abusive des navigateurs et des applications en bloquant les actions qui ne sont pas généralement associées à ces processus.

Interface d'analyse de logiciel anti-programmes malveillants (AMSI)

L'interface AMSI bloque les attaques sans fichier où les malwares sont chargés directement à partir de la mémoire. Sophos Endpoint inclut également une solution propriétaire pour éviter le contournement de la détection AMSI.

Détection du trafic malveillant (MTD)

Détecte les appareils qui communiquent avec des serveurs de commande et contrôle (C2) en interceptant et en analysant le trafic autre que celui des navigateurs, à la recherche de destinations malveillantes.

Défenses adaptatives

Sophos Endpoint s'appuie sur des défenses dynamiques inédites qui automatisent la protection en s'adaptant en temps réel aux adversaires actifs et aux attaques manuelles. Sophos Endpoint identifie et bloque les actions qui ne sont pas nécessairement malveillantes dans un contexte quotidien, mais qui le sont dans le contexte de l'attaque. Cette fonctionnalité répond dynamiquement aux attaques actives et les neutralise, notamment dans les cas où les attaquants peuvent s'être introduits sans déclencher de signaux d'alarme ou sans utiliser de code malveillant.

Protection adaptative contre les attaques

Active dynamiquement des défenses renforcées sur un poste lorsqu'une attaque manuelle est détectée, ce qui entrave l'action de l'adversaire et vous donne plus de temps pour répondre.

Avertissement d'attaque critique

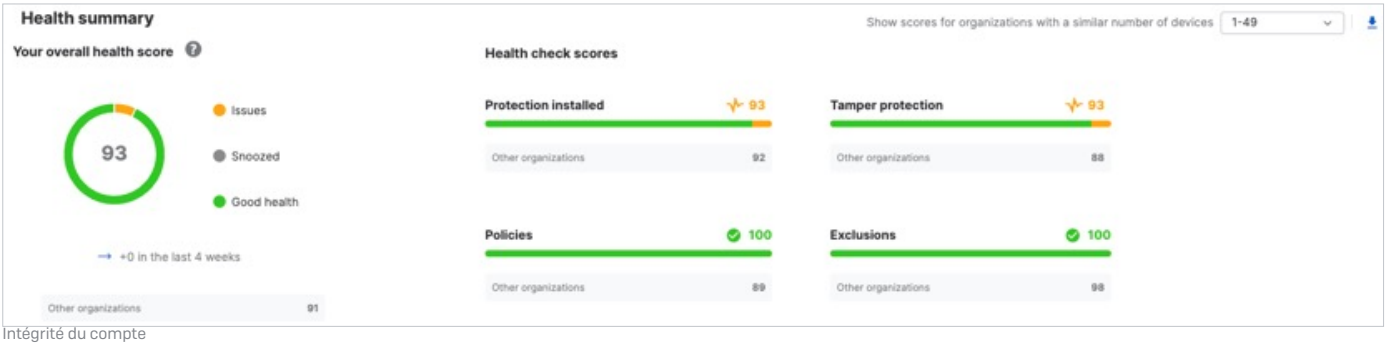
Notifie aux administrateurs les menaces sérieuses en cours sur plusieurs postes, sur la base des détections de menaces à l'échelle de l'entreprise.

	PROTECTION COMPORTEMENTALE	PROTECTION ADAPTATIVE CONTRE LES ATTAQUES	AVERTISSEMENT D'ATTAQUE CRITIQUE
PORTÉE	APPAREIL INDIVIDUEL	APPAREIL INDIVIDUEL	PARC ENTIER
AVANTAGES	Le moteur d'analyse comportementale stoppe les premiers stades des attaques actives	Renforce la sensibilité de la protection pour empêcher toute attaque	Vous alerte en cas d'attaque nécessitant une réponse immédiate
DÉCLENCHEUR	Règles comportementales	Outils de piratage détectés	Indicateurs d'adversaires actifs à fort impact, y compris corrélations et seuils au niveau de l'entreprise
ANALOGIE	« BOUCLIER LEVÉ »	« BOUCLIER RENFORCÉ »	« ALERTE ROUGE »

Défenses adaptatives dans Sophos Endpoint

Identifier les dérives au niveau de la posture de sécurité

Des paramètres de politiques de sécurité, des exclusions ou d'autres facteurs mal configurés peuvent compromettre votre sécurité. La fonction 'Intégrité du compte' identifie toute dérive dans la posture de sécurité et toute erreur de configuration à haut risque, vous permettant de remédier aux problèmes en un seul clic.



Intégrité du compte

Couches de protection supplémentaires (solutions complémentaires)

Sophos ZTNA

Connectez vos utilisateurs à vos applications de manière sécurisée grâce à notre solution ultime qui remplace le VPN. Sophos ZTNA est la seule solution d'accès réseau Zero Trust étroitement intégrée à une protection Endpoint Next-Gen.

Device Encryption

Le chiffrement intégral du disque (FDE) est essentiel compte tenu du nombre d'appareils perdus ou volés chaque jour. Device Encryption intégré dans Sophos Endpoint permet une gestion efficace de BitLocker (Windows) et de FileVault (macOS).

Accélérez la détection, l'investigation et la réponse

Sophos Endpoint bloque automatiquement la plupart des menaces en amont, réduisant ainsi le nombre d'événements à investiguer. Pour les activités suspectes et les menaces qui nécessitent une analyse humaine, Sophos fournit des solutions puissantes pour détecter, investiguer et répondre rapidement à tous les vecteurs d'attaque clés.

Sophos XDR

Sophos XDR (Extended Detection and Response) vous permet de chasser, d'investiguer et de répondre aux activités suspectes et aux attaques multi-étapes à travers l'ensemble de votre environnement. Conçus par des analystes en sécurité pour des utilisateurs de tous niveaux, nos puissants outils alimentés par l'IA générative permettent à tous (des généralistes IT aux analystes SOC de haut niveau) d'investiguer rapidement les menaces et de neutraliser les adversaires.

Sophos XDR propose des intégrations clés en main avec un vaste écosystème de solutions : endpoint, pare-feu, réseau, messagerie, gestion d'identité, productivité, Cloud et sauvegarde, ce qui vous permet d'obtenir un meilleur retour sur investissement de vos outils de sécurité existants.

Pour en savoir plus, consultez Sophos.fr/XDR

Sophos MDR

Pour les entreprises qui ne disposent des ressources nécessaires pour gérer la détection et la réponse aux menaces en interne, Sophos MDR (Managed Detection and Response) est un service 24/7 assuré par une équipe de haut vol spécialisée dans l'analyse de sécurité, la chasse aux menaces et la réponse aux incidents. Sophos MDR exploite la télémétrie des technologies de sécurité à la fois de Sophos et de tiers pour identifier et neutraliser toutes les menaces, même les plus sophistiquées.

Sophos MDR vous rejoint là où vous êtes, avec plusieurs niveaux de service et modes de réponse pour répondre aux besoins de votre entreprise, et une compatibilité avec vos outils et technologies existants.

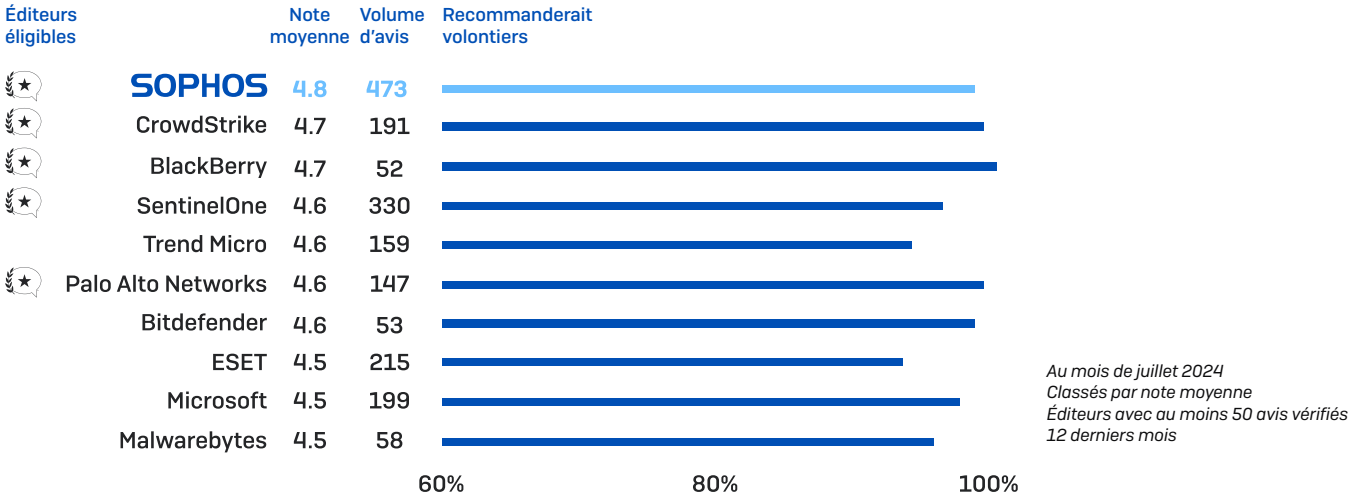
Pour en savoir plus, consultez Sophos.fr/MDR

	Sophos Endpoint	Sophos XDR	Sophos MDR
Protection Next-Gen contre les menaces Protection web, anti-malware grâce au Deep Learning et à l'IA	✔	✔	✔
Blocage des activités malveillantes Défenses adaptatives anti-ransomware et anti-exploit	✔	✔	✔
Réduction de l'exposition aux menaces Fonctionnalités DLP et contrôles du Web, des périphériques et des applications	✔	✔	✔
Détection et réponse Outils puissants d'investigation et de réponse aux menaces		✔	✔
Visibilité sur les surfaces d'attaque clés Intégration de technologies Sophos et tierces		✔	✔
Service MDR (Managed Detection and Response) Surveillance des menaces et réponse aux incidents par des experts, 24/7			✔

La solution de protection Endpoint la mieux notée et la plus évaluée

Dans le rapport '2024 Voice of the Customer for Endpoint Protection Platforms' de Gartner, Sophos a reçu le plus grand nombre d'avis parmi tous les fournisseurs et a obtenu une note de 4,8 sur 5. Sophos a également été nommé '2024 Customers' Choice' dans les 11 secteurs d'activité inclus dans le rapport.

Plateformes de protection Endpoint



Au mois de juillet 2024
Classés par note moyenne
Éditeurs avec au moins 50 avis vérifiés
12 derniers mois

Découvrez pourquoi les clients choisissent Sophos Endpoint

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

Gartner

Sophos nommé Leader dans le Magic Quadrant™ 2024 de Gartner® dans la catégorie EPP (Endpoint Protection Platforms) dans 15 rapports consécutifs.

SE Labs

Sophos obtient régulièrement les meilleurs résultats en matière de protection dans des tests de sécurité Endpoint indépendants.

G2 Leader

Sophos nommé Leader dans les rapports G2 Grid® Winter 2025 dans les catégories Endpoint Protection Suites, EDR, XDR, Firewall Software et MDR.

IDC

Sophos nommé Leader par l'IDC MarketScape 2024 dans la catégorie 'Worldwide Modern Endpoint Security for Small and Midsize Businesses'

Essai gratuit

Évaluation gratuite de 30 jours sur sophos.fr/endpoint

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

2025-03-04 SB-FR (NP)

SOPHOS