SOPHOS

Guide d'achat de la sécurité Endpoint

Plus les cybermenaces se complexifient, plus la pression pour trouver la solution Endpoint adaptée s'accentue. Cependant, avec un marché de la sécurité saturé de solutions multiples et variées, chacune prétendant être la meilleure, il est de plus en plus difficile de prendre une décision éclairée au nom de votre entreprise.

Ce document a été conçu pour vous éclairer et vous guider dans le choix de votre sécurité Endpoint en vous présentant les fonctionnalités indispensables, ainsi que tous les paramètres nécessaires pour assurer une protection efficace contre les menaces avancées d'aujourd'hui. Grâce à ces informations, vous serez plus à même de prendre la bonne décision pour votre entreprise.

Un livre blanc Sophos. Juin 2024

Le paysage actuel des cybermenaces

Notre enquête indépendante, réalisée auprès de 3 000 responsables de l'informatique/cybersécurité répartis dans 14 pays, a montré que, dans les faits, il existe actuellement un système à deux vitesses, avec des attaquants et des défenseurs qui progressent à des rythmes différents. Ralentis par de nombreux vents contraires, les défenseurs prennent du retard tandis que les adversaires, de leur côté, accélèrent.

L'évolution de l'économie de la cybercriminalité

L'un des changements les plus importants dans le paysage des menaces de ces dernières années a été la transformation de l'économie cybercriminelle en une véritable industrie, avec un réseau de services support et des approches opérationnelles bien établies et professionnelles.

Alors que les entreprises technologiques ont évolué vers des offres « as-a-service », l'écosystème de la cybercriminalité en a fait de même. Cela a abaissé les barrières et facilite l'entrée de cybercriminels potentiels et permis aux acteurs malveillants d'accélérer le volume, la vitesse et l'impact de leurs attaques.

Résultat : les adversaires peuvent désormais lancer un large éventail d'attaques sophistiquées, et ce à grande échelle. 94 % des entreprises ont subi une cyberattaque en 2022. Si le ransomware apparaît comme l'attaque la plus signalée, les entreprises ont également dû faire face à d'autres types de menaces, notamment :[1]

27 %	**27 %**	**26 %**
Email malveillant	Phishing (y compris spearphishing)	Exfiltration de données (par l'attaquant)
24 %	**24 %**	**21 %**
Cyber extorsion	Compromission de la messagerie professionnelle	Malwares mobiles
18 %	**24 %**	**14 %**
Cryptomineurs	Déni de service (DDoS)	Wipers

Consultez notre rapport L'état de la cybersécurité en 2023 : l'impact des cyberattaques sur les entreprises, pour en savoir plus.

Les ransomwares continuent d'empoisonner les entreprises

En matière de ransomware, 59 % des entreprises affirment avoir été victimes d'une attaque au cours des douze derniers mois.

2020	2021	2022	2023	2024
51 %	37 %	66 %	66 %	59 %

Au cours de l'année passée, votre organisation a-t-elle été touchée par un ransomware ?
Oui. n=5 000 (2024) n=3 000 (2023), 5 600 (2022), 5 400 (2021), 5 000 (2020)

Si le taux d'attaques signalé en 2024 a diminué par rapport au chiffre de 2023, le chiffrement des données par un ransomware reste élevé : les cybercriminels parvenant à chiffrer les données dans 70 % des attaques.

Les ransomwares coûtent également plus que jamais aux entreprises, qui font état d'un coût de rétablissement moyen de 2,73 million de dollars, alors qu'il était de 1,82 million de dollars en 2023.[2]

Pour en savoir plus, vous pouvez lire notre rapport annuel sur les ransomwares 'L'état des ransomwares 2024', qui vous aidera à mieux connaître les défis rencontrés par les entreprises en 2024, notamment la fréquence, le coût et la cause première des attaques.

1 L'état de la cybersécurité en 2023 : l'impact des cyberattaques sur les entreprises, Sophos — Une étude indépendante menée entre janvier et février 2023 auprès de 3 000 responsables IT/cybersécurité répartis dans 14 pays.

2 L'état des ransomwares 2024, Sophos — Une étude indépendante et agnostique réalisée entre janvier et février 2024, auprès de 5 000 responsables IT/cybersécurité dans 14 pays.

Les approches traditionnelles conduisent à des résultats médiocres en matière de sécurité

Ces dernières années, les entreprises et autres organisations ont connu de profonds changements. Leurs utilisateurs peuvent travailler en présentiel, à distance ou se déplacer régulièrement entre leurs clients et leurs partenaires. Les données de l'entreprise ne sont plus uniquement conservées sur site. Elles peuvent être stockées en local, dans le cloud et sur les systèmes des utilisateurs, tout en restant accessibles localement et à distance pour répondre aux besoins des collaborateurs géographiquement dispersés. En termes de cybersécurité, il est donc devenu aujourd'hui contreproductif de continuer à suivre les approches traditionnelles, aux résultats bien insuffisants.

Parmi les problèmes rencontrés par les équipes de sécurité IT, voici les plus courants :

- **Manque de compétences :** le recrutement de talents en la matière continue d'être un véritable défi pour les entreprises. Un manque d'expérience signifie que les employés peuvent ne pas avoir les compétences nécessaires pour déterminer si une alerte de sécurité est malveillante ou bénigne.
- **Surcharge d'alertes :** les techniciens sont submergés par un nombre excessif d'alertes, provenant d'une multitude de systèmes, et souvent, ils ne savent pas comment les prioriser, risquant ainsi de passer à côté de signaux clés, indicateurs d'une attaque.
- **Données cloisonnées :** comme les signaux/alertes de menace sont limités à certaines technologies, les équipes IT ne bénéficient pas d'une vue globale pour remédier rapidement aux alertes ou incidents malveillants.
- **Manque d'intégration :** les outils de sécurité ne s'intègrent pas les uns aux autres ou à l'infrastructure informatique d'une entreprise, ce qui accroît la complexité.
- **Processus manuels :** les équipes IT passent de nombreuses heures à corréler les événements, les journaux et les informations pour comprendre ce qui se passe. Tout ce travail retarde la capacité à identifier l'attaque et à y répondre.
- **Manque de réactivité :** en raison des problèmes mentionnés ci-dessus, de nombreuses équipes IT sont en position désavantageuse ; elles ne réagissent aux menaces qu'une fois les dommages causés, au lieu de les arrêter plus tôt dans la chaîne d'attaque.
- **Travail dans l'urgence :** les efforts quotidiens pour neutraliser les menaces empêchent les améliorations à long terme. Lorsque l'équipe IT est en train « d'éteindre le feu », elle n'est pas en mesure de s'occuper du plus important : identifier la cause première de l'incident ou tenir un registre précis sur l'attaque et les mesures prises. Les problèmes structurels de fond ne sont pas résolus et persistent.
- **Données distribuées :** les utilisateurs et les appareils sont partout. Les données sont donc, elles aussi, omniprésentes, que ce soit en local, dans le cloud, sur les multiples appareils — et accessibles localement et via des solutions d'accès à distance.

L'un des moyens de relever la plupart de ces défis consiste à déployer une solution de protection Endpoint de premier ordre.

Les indispensables d'une bonne sécurité Endpoint

Une solution de sécurité Endpoint moderne et efficace doit travailler pour vous et avec vous, en adaptant vos défenses en fonction de l'attaque. Elle doit, avant tout, reposer sur un principe de prévention afin de :

Réduire l'exposition aux menaces : bloquer les contenus malveillants et les menaces Web, et contrôler l'accès aux applications, aux sites Internet, aux périphériques, etc.

Bloquer les activités malveillantes : empêcher les techniques et les exploits que les développeurs malveillants et les ransomwares utilisent pour atteindre leurs objectifs, en identifiant l'activité en question et en la bloquant avant qu'elle ne cause de dommages.

Faciliter des réponses adaptées et automatisées : vos défenses devraient automatiquement répondre aux menaces et s'adapter aux comportements des attaquants. Cela permet non seulement d'entraver leurs actions, mais aussi d'alerter votre équipe de leur présence et de lui laisser un temps précieux pour répondre.

Servir d'outil pour chasser les menaces (en interne ou managé pour vous) : des signaux de haute qualité enrichis d'informations de sécurité peuvent considérablement accélérer la capacité à détecter et à répondre aux menaces. Plus ces informations seront détaillées, plus la résolution sera rapide.

Garantir des résultats optimaux

Alors que nous venons de voir ce qu'une solution Endpoint efficace doit apporter d'un point de vue fonctionnel, il est essentiel de voir comment elle peut soutenir votre entreprise de manière plus globale. Sa finalité est de garantir des résultats optimaux en matière de sécurité.

Réduction des cyber risques

Une protection Endpoint solide réduit votre risque cyber et vous protège contre une multitude de menaces.

Approche axée sur la prévention

Plus l'attaque sera stoppée tôt en amont, moins il y aura de travail à effectuer (si ce n'est aucun). Une solution supérieure utilise plusieurs couches de protection pour lutter contre les cybermenaces et les attaques visant tous les types de systèmes : postes de travail, ordinateurs portables, mobiles et serveurs. Elle sécurise ces systèmes et leurs données contre les malwares, les virus, les ransomwares et toute autre activité malveillante.

Identifier les dérives au niveau de la posture de sécurité

La posture de sécurité va dériver au fil du temps, et ce, pour un certain nombre de raisons. Une étude récente réalisée auprès de fournisseurs a montré que la mauvaise configuration des outils de sécurité était identifiée comme le principal risque de sécurité par les responsables informatiques en 2023.[2]

Privilégiez donc les solutions de sécurité Endpoint qui évaluent en permanence votre posture de sécurité et optimisent votre configuration. Cette approche automatisée est essentielle pour obtenir une posture de sécurité solide, réduire votre cyber risque et vous éviter le casse-tête des configurations manuelles.

Gestion optimisée

Une console de gestion centralisée permet aux administrateurs IT de surveiller et de gérer les paramètres de sécurité, les politiques, les exclusions et les alertes sur l'ensemble des systèmes d'extrémité à partir d'un seul et même endroit. Cela simplifie la gestion globale de la sécurité, réduit les risques d'erreur de configuration et garantit une protection cohérente. Certaines consoles de gestion centralisée vont encore plus loin en vérifiant automatiquement l'état de votre posture et en signalant toute activité ou modification de politique susceptible de la compromettre.

Accélérer la détection et la réponse

Chaque seconde compte lorsqu'un adversaire se trouve dans votre environnement. Une protection Endpoint de haut niveau qui repose sur le principe de prévention réduit la quantité de bruit et émet des alertes « haute fidélité ». Les technologies EDR (Endpoint Detection and Response) et XDR (Extended Detection and Response) peuvent être utilisées pour analyser ces alertes.

Certaines solutions vont encore plus loin en exploitant l'intelligence artificielle (IA) et les renseignements sur les menaces afin de prioriser automatiquement les détections. Ces solutions permettent à votre équipe de mieux gérer et optimiser leur temps, et d'accélérer la réponse humaine aux menaces.

Efficacité IT accrue

Dans les faits, 64 % des entreprises souhaitent que leurs équipes IT consacrent moins de temps à lutter contre les cyberattaques et plus de temps aux questions stratégiques.[3] Une sécurité Endpoint automatisée et conviviale les aide à atteindre cet objectif.

Les solutions haut de gamme bloquent et nettoient automatiquement la majorité des menaces en amont. Cela libère des ressources et permet ainsi aux équipes IT de se consacrer à des projets plus stratégiques pour l'entreprise. Des technologies telles que XDR permettent de réduire la charge de travail liée aux signaux, débloquant du temps pour d'autres initiatives plus importantes.

Cette efficacité accrue permet la transition vers une cybersécurité proactive, et non plus réactive. Elle offre aux équipes IT le temps requis pour détecter les menaces avant que des dommages, potentiellement durables et persistants, ne soient causés. Ce qui réduit également les cyber risques.

2 L'état des ransomwares 2024, Sophos — Une étude indépendante et agnostique réalisée entre janvier et février 2024, auprès de 5 000 responsables IT/cybersécurité dans 14 pays.

3 L'état de la cybersécurité en 2023 : l'impact des cyberattaques sur les entreprises, Sophos - Une étude indépendante menée entre janvier et février 2023 auprès de 3 000 responsables informatiques et responsables de la cybersécurité répartis dans 14 pays.

Optimiser son retour sur investissement

Une cybersécurité solide doit protéger les entreprises des conséquences financières et opérationnelles qu'un incident de sécurité majeur pourrait avoir.

C'est pourquoi investir dans une sécurité Endpoint supérieure est indispensable. La prévention, lorsqu'elle est bien conçue et menée, revient bien moins chère que les coûts de réparation. Une protection Endpoint solide bloque d'emblée la majorité des menaces, réduisant ainsi le risque de se retrouver victime d'une attaque et d'avoir à subir les coûts qui en résultent.

En outre, les solutions haut de gamme peuvent s'intégrer/communiquer avec vos produits actuels afin d'étendre votre protection, de minimiser la complexité et de faire en sorte que vos technologies déjà en place (messagerie, pare-feu, réseau, gestion d'identité et cloud) fonctionnent plus intelligemment et plus efficacement que jamais.

Tous ces avantages améliorent le retour sur investissement de votre cybersécurité tout en réduisant votre coût total de possession.

Un meilleur positionnement vis-à-vis des assureurs

Ces dernières années, les primes de cyberassurance ont augmenté de manière significative, et les conditions requises pour pouvoir y prétendre se sont durcies. Les assureurs exigent des cyber contrôles plus rigoureux. Dans les faits, 95 % des entreprises ayant souscrit une assurance l'année dernière ont déclaré que la qualité de leurs défenses avait une incidence directe sur leur assurabilité[4].

La clé pour optimiser votre assurabilité est de limiter votre cyber risque au maximum. Investir dans des défenses solides, y compris des services de sécurité 24/7 et des outils de détection et de réponse de pointe, offre de multiples avantages en matière d'assurance :

1. Facilite l'obtention d'une couverture d'assurance cyber (autrement dit, améliore la capacité à être assuré)
2. Contribue à réduire les primes et à améliorer les conditions générales
3. Réduit la probabilité d'un sinistre — et les primes plus élevées qui en résultent
4. Réduit le risque de non-indemnisation en cas d'incident

Les meilleures technologies de sécurité Endpoint comprennent des fonctions de détection et de réponse, alors assurez-vous que les fournisseurs que vous sélectionnez les intègrent dans leur offre. La technologie EDR (Endpoint Detection and Response) est désormais une condition pré-requise par les assureurs et les entreprises qui n'en disposent pas ont généralement du mal à souscrire une police de cyberassurance.

Les services qui optimisent la détection et la réponse et minimisent ainsi le risque d'incident cyber sont considérés comme le « standard de référence » par les cyberassureurs. En effet, les entreprises qui utilisent ces services, et plus particulièrement les services MDR (Managed Detection and Response) sont souvent considérées comme des clients de « première classe » par les assureurs, car elles présentent le niveau de risque le plus faible.

Cela dit, vous pouvez faire appel à des fournisseurs offrant une mise à niveau transparente de votre solution Endpoint vers un service entièrement managé 24/7 pour la chasse aux menaces, et la détection ou réponse aux incidents, qui s'intègre à vos produits actuels et aux contrôles de sécurité tiers.

5 Le rôle critique des cyberdéfenses de première ligne lors du recours à la cyberassurance — Sophos.

Évaluer la sécurité Endpoint : Les 10 questions à poser

Maintenant que vous avez une idée plus précise des caractéristiques que doit présenter une solution Endpoint de pointe, voici quelques questions à poser aux fournisseurs potentiels.

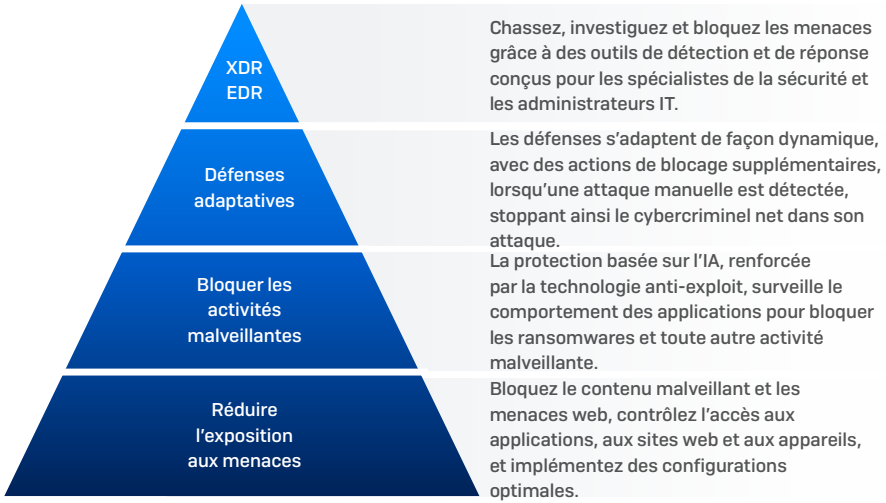
1. Votre produit adopte-t-il une approche de prévention multicouche ? Ou s'appuie-t-il avant tout sur une approche de détection ? Quelles sont les fonctions spécifiques au cœur de sa technologie ?
2. Votre produit dispose-t-il de fonctionnalités permettant de détecter et de rectifier automatiquement toute dérive de la posture de sécurité ? Peut-il signaler toute modification des paramètres de la politique de sécurité susceptible d'accroître les risques ?
3. Le produit répond-il automatiquement aux menaces ? Peut-il automatiquement nettoyer une menace et répondre à un incident ?
4. Votre produit dispose-t-il de défenses qui s'adaptent automatiquement lorsqu'une attaque active "manuelle" (ou « hands-on-keyboard ») est détectée ?
5. Votre produit dispose-t-il de solides fonctionnalités anti-ransomware et anti-exploit, dont une protection en temps réel contre les attaques de ransomware distant ? Ces fonctionnalités sont-elles activées par défaut ? Ces fonctionnalités doivent-elles être activées et entraînées avant de fonctionner dans votre environnement ?
6. Combien de consoles faut-il pour gérer votre produit ? La ou les consoles sont-elles hébergées dans le cloud ou nécessitent-elles une installation sur site ?
7. Votre produit permet-il une transition transparente vers les technologies EDR/XDR grâce à la même console de gestion et au même agent sur le système d'extrémité/serveur ?
8. La fonction XDR intègre-t-elle des alertes provenant de contrôles de sécurité natifs et tiers afin d'obtenir une vue d'ensemble de mon environnement ?
9. Le produit permet-il une mise à niveau transparente vers un service de chasse aux menaces, de détection et de réponse aux incidents entièrement managé, 24 h/24 et 7 j/7, capable de s'intégrer à mes produits actuels et aux contrôles de sécurité tiers ?
10. Le fournisseur peut-il attester de la validation de son approche de sécurité Endpoint par des organismes de test ou des analystes indépendants, ou encore des témoignages clients ?

L'approche Sophos

Examinons maintenant la vision de Sophos en matière de protectionEndpoint. Sophos Endpoint offre une protection inégalée contre les cyberattaques sophistiquées. Une protection anti-ransomware imperméable doublée d'une approche de défense en profondeur bloque la plus large gamme de menaces avant qu'elles n'affectent vos systèmes. Des outils EDR et XDR puissants permettent à votre équipe de chasser, d'investiguer et de répondre aux menaces avec rapidité et précision.

Approche axée sur la prévention

Sophos Endpoint adopte une approche globale pour protéger tous les postes de travail et ne s'appuie pas uniquement sur une seule technique de sécurité. En bloquant plus de menaces en amont, les équipes informatiques ont moins d'incidents à investiguer et à résoudre.



Réduire l'exposition aux menaces

Sophos Endpoint réduit votre exposition aux menaces et la capacité des attaquants à pénétrer dans votre environnement. Il bloque les menaces Web et les contenus malveillants, et vous permet de contrôler l'accès aux applications, aux sites Internet et aux appareils périphériques.

Bloquer les menaces Web et contrôler l'accès à Internet

Les menaces basées sur le Web sont nombreuses et variées. Les entreprises utilisent souvent des pare-feux Next-Gen afin de protéger leurs utilisateurs travaillant dans leurs locaux contre le phishing, les sites Internet malveillants et toute autre menace Web. Bien que cette pratique sécurise les postes sur le réseau de l'entreprise, ces mêmes systèmes peuvent être utilisés à la maison, sur la route, dans des lieux publics, etc., où aucun pare-feu ne les protège.

Sophos Endpoint bloque l'accès aux sites de phishing et aux sites Internet malveillants en analysant les fichiers, les pages Web et les adresses IP. Il garantit que les systèmes sont protégés en permanence contre les menaces, quel que soit l'endroit où ils se trouvent.

De plus, les SophosLabs et l'équipe Sophos MDR fournissent des renseignements sur les menaces en temps réel afin de protéger les clients Sophos contre les menaces émergentes.

Contrôler le Web, les périphériques et les applications

Sophos vous permet de restreindre les activités des systèmes d'extrémité. Ces contrôles sont généralement mis en place dans le cadre de la politique d'utilisation acceptable de l'entreprise.

Le premier contrôle consiste à surveiller ou à bloquer l'accès à certaines catégories de sites Internet (jeux d'argent, réseaux sociaux, etc.). Sophos Endpoint vous permet de surveiller et de bloquer des catégories de sites Internet, et cette règle s'applique aussi bien au sein qu'en dehors du ou des réseaux de l'entreprise.

Contrôler l'accès aux supports amovibles ou à d'autres périphériques peut davantage réduire votre surface d'attaque. Pensez à toutes les fois où un utilisateur branche une imprimante ou une clé USB ou bien recharge son téléphone portable à partir d'un port USB. L'une ou l'autre de ces actions est-elle autorisée ? Cette fonctionnalité permet non seulement d'empêcher un vecteur d'attaque d'introduire un code malveillant sur un système, mais aussi de bloquer l'exfiltration des données de l'entreprise.

Autre catégorie importante à prendre en compte : les applications. Le contrôle des applications permet de bloquer l'exécution d'applications ou de plug-ins de navigateur sur les appareils de l'entreprise. Comme pour l'exfiltration de données, songez à des applications telles que OneDrive ou Google Drive pour le stockage dans le cloud. Réfléchissez également aux logiciels torrent, au navigateur TOR, etc., et si ceux-ci devraient être autorisés ou non sur vos postes de travail. Il existe un large éventail de plug-ins pour les navigateurs Web. Si bon nombre d'entre eux ont des utilisations légitimes et bénéfiques, d'autres n'en ont aucune.

Bloquer les activités malveillantes

La couche de défense suivante implique l'utilisation de l'intelligence artificielle, de l'analyse comportementale, de technologies anti-ransomware et anti-exploit, ainsi que d'autres technologies pour stopper les menaces rapidement avant qu'elles ne s'aggravent.

Sophos utilise une protection « AI-first », en commençant par la classification des exécutables par IA. Elle repose sur un modèle formé sur des millions de bons et mauvais exécutables. Ce modèle permet d'identifier rapidement et efficacement les exécutables malveillants en fonction de leurs propriétés et ne nécessite aucune signature.

Protection anti-ransomware imperméable

Sophos Endpoint est la protection endpoint zero-touch la plus robuste contre les ransomwares locaux et distants. Elle inclut la technologie avancée CryptoGuard qui détecte tout indice de chiffrement, quelle qu'en soit la source. Cette approche universelle bloque les nouvelles variantes et les ransomwares locaux et distants. Elle inspecte en temps réel les modifications apportées au contenu des fichiers afin de détecter le chiffrement malveillant et bloque les ransomwares distants s'exécutant sur un autre appareil et qui tentent de chiffrer les fichiers sur le réseau. Les fichiers chiffrés sont automatiquement restaurés vers un leur état d'origine non chiffré, indépendamment de la taille ou du type de fichier, minimisant ainsi tout impact sur la productivité de l'entreprise. Sophos Endpoint protège également le MBR (Master Boot Record) contre le chiffrement utilisé dans certaines attaques de ransomware.

Anti-exploit

La technologie anti-exploit bloque les comportements et les techniques sur lesquels les attaquants s'appuient pour compromettre les appareils, voler des identifiants et distribuer des malwares. Sophos déploie de nouvelles approches anti-exploit sur les appareils pour toutes les applications. Prêt à l'emploi dès l'installation, Sophos s'appuie sur la protection de base offerte par Microsoft Windows avec pas moins de 60 mesures de protection anti-exploit préconfigurées, propriétaires et adaptées. Résultat : Sophos maintient votre entreprise parfaitement sécurisée contre les attaques sans fichier et les exploits de type « zero-day », en bloquant les techniques employées tout au long de la chaîne d'attaque.

Défenses adaptatives

Ces défenses dynamiques supplémentaires sont une première dans l'industrie. Elles fournissent une protection automatisée de niveau supérieur qui s'adapte au contexte de l'attaque. Sophos Endpoint identifie et bloque les actions qui, dans un contexte quotidien, ne seraient pas malveillantes en soi, 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.

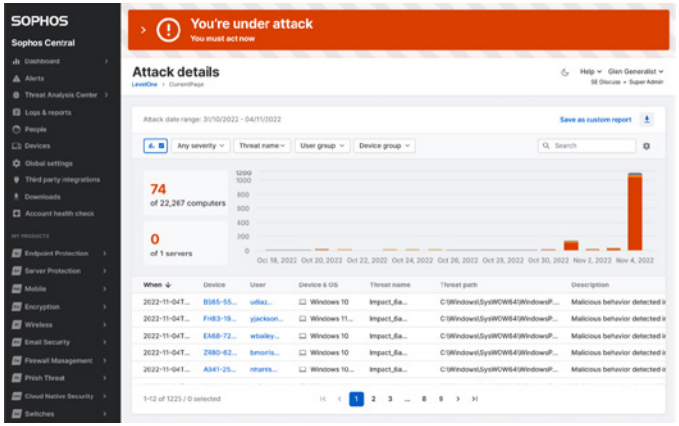
	PROTECTION COMPORTEMENTALE	PROTECTION ADAPTATIVE CONTRE LES ATTAQUES	AVERTISSEMENT D'ATTAQUE CRITIQUE
PORTÉE	APPAREIL INDIVIDUEL	APPAREIL INDIVIDUEL	APPAREIL INDIVIDUEL
AVANTAGES	Le moteur d'analyse comportementale stoppe les premiers stades des attaques actives.	Renforce la sensibilité de la protection pour empêcher tout dommage	Alerte le client en cas d'attaque nécessitant une réponse immédiate
DÉCLEN-CHEUR	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 »

Protection adaptative contre les attaques

La protection adaptative contre les attaques met en œuvre dynamiquement des défenses renforcées au niveau d'un système endpoint lorsqu'une attaque « manuelle » est détectée. Ces défenses ont plusieurs effets : empêcher l'attaquant de poursuivre ses actions, réduire la surface d'attaque, contenir et neutraliser l'attaque, et gagner du temps pour répondre.

Avertissement d'attaque critique

Un avertissement d'attaque critique vous alerte d'une attaque grave au niveau du parc IT si une activité adverse est détectée sur plusieurs postes ou serveurs de votre environnement avec des indicateurs supplémentaires à fort impact. Il s'agit d'une alerte rouge, qui signifie que vous êtes attaqué. Une technologie automatisée vous informe de la situation, en vous fournissant le contexte et le détail de l'attaque. Vous pouvez répondre à l'aide de Sophos XDR, demander assistance auprès de votre partenaire ou faire appel à l'équipe de réponse aux incidents de Sophos pour vous aider à traiter la menace.



Réduire le coût total de possession de la cybersécurité

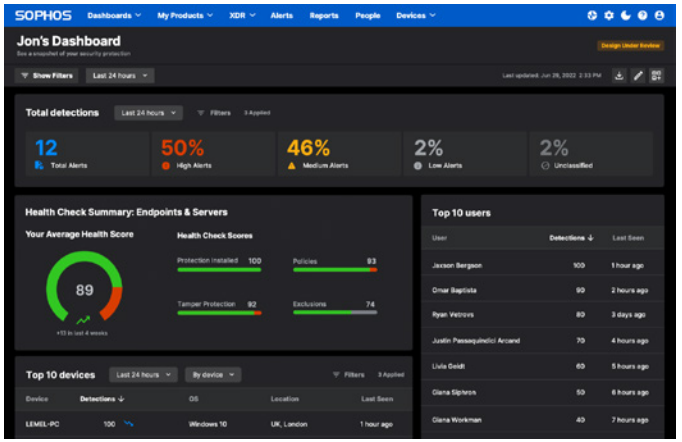
Aujourd'hui, la plupart des équipes informatiques et de sécurité sont surchargées. Sophos Endpoint leur offre deux atouts majeurs : l'automatisation et le gain de temps. Tout ce qui pourra être automatisé, réduit ou supprimé de leur charge de travail leur permettra de se consacrer à d'autres tâches et d'autres projets plus stratégiques.

Sophos Central est une plateforme d'administration basée dans le cloud, d'où vous pouvez gérer tous vos produits Sophos (postes, serveurs, mobiles, pare-feux, Switch, points d'accès, messagerie et cloud), dont Sophos Endpoint. Depuis un seul et même endroit, vous pouvez créer et gérer vos politiques de sécurité, visualiser les détections et les alertes, examiner les menaces potentielles et y remédier, et effectuer d'autres actions sur l'ensemble de vos produits Sophos.

Les technologies de protection recommandées par Sophos sont toutes activées par défaut, ce qui facilite l'installation et vous permet de bénéficier immédiatement des paramètres de sécurité les plus puissants, sans qu'aucun réglage ne soit nécessaire. Un contrôle granulaire est également disponible si nécessaire.

Identifier les dérives au niveau de la posture de sécurité

Avec le temps, la posture de sécurité d'une entreprise aura tendance à s'éloigner de son état de conformité ou de configuration optimale. Les paramètres de politique mal configurés, les exclusions et d'autres facteurs sont autant de risques de sécurité. La fonction « Intégrité du compte » identifie toute dérive dans la posture de sécurité et toute erreur de configuration à haut risque, permettant aux administrateurs de remédier aux problèmes en un seul clic.

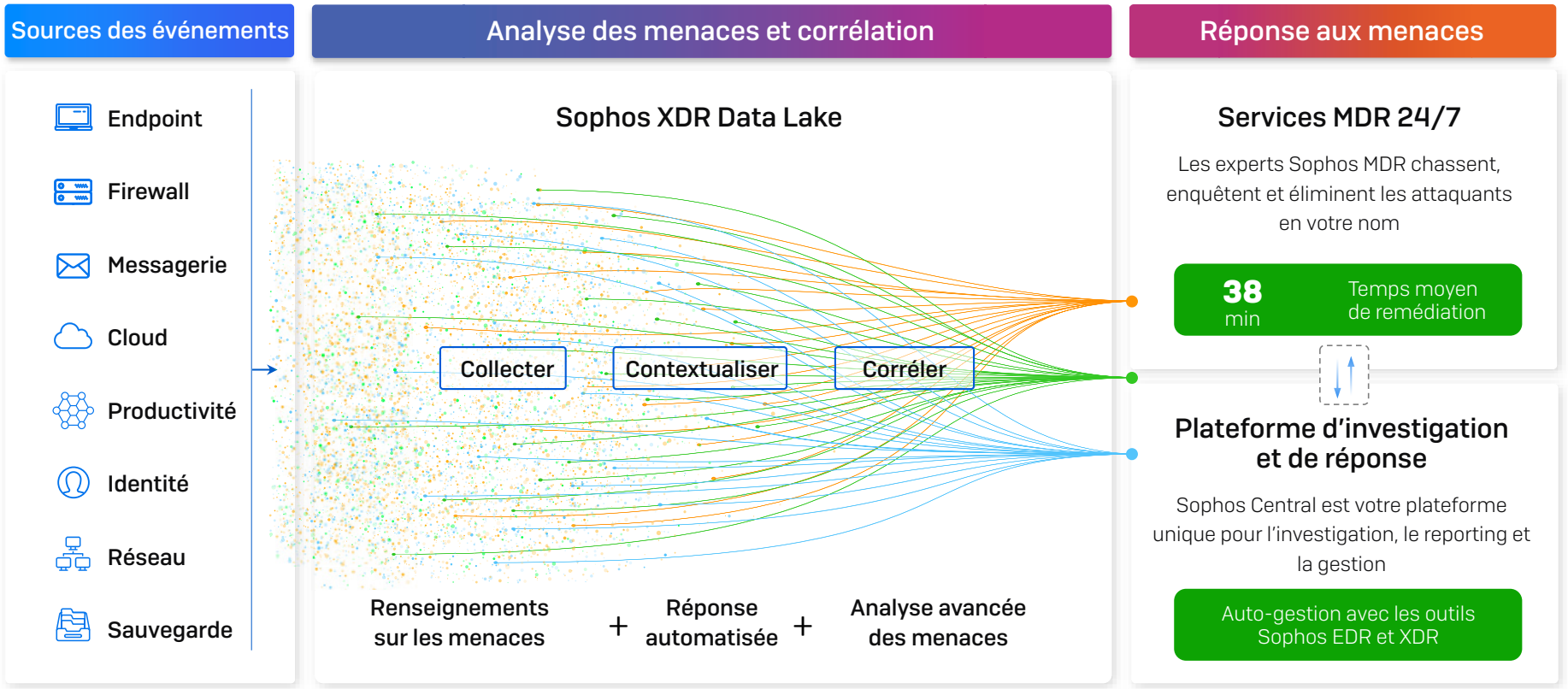


Sécurité Synchronisée

Les solutions Sophos fonctionnent mieux ensemble. Sophos Endpoint partage les informations de sécurité avec Sophos Firewall, Sophos ZTNA, et d'autres produits pour une visibilité accrue sur les menaces et sur l'utilisation des applications. La Sécurité Synchronisée de Sophos isole automatiquement les appareils compromis pendant la durée du nettoyage, puis rétablit l'accès au réseau une fois la menace neutralisée, le tout sans intervention de l'administrateur.

Accélérer la détection et la réponse : EDR, XDR et MDR

L'approche de Sophos basée sur la prévention bloque et nettoie automatiquement le plus grand nombre possible de menaces en amont. Les équipes IT et de sécurité ont ainsi moins de détections à investiguer par la suite.



L'approche de Sophos en matière de prévention, de détection et de réponse.

Sophos Endpoint Detection and Response (EDR)

Sophos intègre de puissantes fonctionnalités de détection et de réponse aux capacités de prévention de Sophos Endpoint. Cela permet de chasser, d'analyser et de répondre aux activités suspectes aussi bien sur les postes que sur les serveurs. Les détections sont analysées et priorisées par l'IA, pour vous aider à définir où consacrer votre temps et votre énergie. Les opérateurs peuvent accéder aux appareils à distance pour investiguer les problèmes, installer et désinstaller des logiciels, et remédier aux incidents éventuels.

Sophos Extended Detection and Response (XDR)

Pour les entreprises qui recherchent des fonctionnalités de détection et de réponse aux menaces plus complètes, Sophos XDR vous permet de chasser, d'investiguer et de répondre aux activités suspectes et aux attaques multi-étapes à travers l'ensemble de votre environnement. Conçu par des analystes de la sécurité pour des analystes de la sécurité, c'est le seul outil sur le marché qui fusionne la télémétrie native de Sophos avec des contrôles de sécurité tiers afin d'accélérer la détection et la réponse. 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.

Sophos Managed Detection and Response (MDR)

Pour les entreprises qui ne disposent des ressources nécessaires pour gérer la détection et la réponse aux menaces en interne, Sophos MDR est un service 24/7 assuré par une équipe d'élite en chasse aux menaces et en réponse aux incidents. Sophos MDR exploite la télémétrie des contrôles de sécurité à la fois de Sophos et de tiers pour identifier et neutraliser toutes les menaces, même les plus sophistiquées et les plus complexes.

Sophos XDR et Sophos MDR s'adaptent à votre situation actuelle, en s'intégrant à vos solutions déjà en place — messagerie, pare-feu, réseau, gestion d'identité et cloud — ce qui vous permet de jouir d'un meilleur retour sur investissement.

Contrat de services Sophos de réponse aux incidents

Le Contrat de services Sophos de réponse aux incidents est un abonnement annuel qui permet aux clients Endpoint, EDR et XDR d'accéder rapidement à une équipe d'experts en réponse aux incidents, avec des conditions de service préétablies, pour stopper rapidement les attaques actives et vous permettre de reprendre vos activités normales.

Pourquoi choisir Sophos

Sophos est un leader mondial et un innovateur dans le domaine des solutions de cybersécurité avancées, qui comprend des services managés de détection et réponse (MDR) et de réponse aux incidents, ainsi qu'un vaste portefeuille de technologies de sécurité qui protègent les systèmes endpoint, les réseaux, les messageries et le cloud contre les cyberattaques. Sophos est l'un des plus grands fournisseurs de cybersécurité et protège aujourd'hui plus de 550 000 entreprises et plus de 100 millions d'utilisateurs dans le monde contre les adversaires actifs, les ransomwares, le phishing, les malwares, etc. Cette visibilité inégalée sur le paysage des menaces permet d'obtenir des renseignements sur les menaces inégalés, utilisés pour améliorer les capacités défensives des produits et des services Sophos pour tous les clients.

Tests indépendants

Des tests indépendants réputés sont un outil important pour aider les entreprises à prendre des décisions éclairées concernant leurs solutions technologiques et leurs investissements en matière de sécurité. Cependant, à mesure que les attaques augmentent en volume et en complexité, des résultats significatifs ne peuvent être obtenus que lorsque les tests reflètent la réalité du terrain à laquelle les organisations sont confrontées aujourd'hui.

SE Labs

SE Labs est l'un des rares organismes indépendants spécialisés dans les tests de sécurité du secteur à simuler les outils d'attaque modernes et les tactiques, techniques et procédures (TTP) que les cybercriminels et les pentesteurs utilisent actuellement dans le monde réel.

Dans le dernier rapport de SE Labs sur la sécurité Endpoint (janvier à mars 2024), Sophos s'impose à nouveau comme la meilleure protection sur le marché, en obtenant des notes AAA dans tous les domaines dans les deux catégories Enterprise et SMB. Les rapports du premier trimestre 2024 de SE Labs sont disponibles ici :

Sécurité Endpoint : Enterprise | Endpoint Security: Small Business

Évaluations MITRE Engenuity ATT&CK

Sophos a excellé lors de la série d'évaluations 2023 MITRE Engenuity ATT&CK Evaluations for Enterprise (Turla). Sophos XDR a détecté 99 % des comportements malveillants dans l'évaluation (identification de 141 sous-étapes sur 143 dans l'attaque adverse). Sophos XDR a également démontré sa capacité à fournir aux équipes de sécurité un contexte détaillé sur le comportement de l'attaquant (ce qu'il fait, pourquoi il le fait et comment il le fait), enregistrant une couverture analytique riche pour 98 % des sous-étapes comprises dans la série d'évaluation.

Les évaluations MITRE Engenuity ATT&CK comptent parmi les tests de sécurité indépendants les plus respectés au monde, en grande partie grâce à la construction et à l'émulation réfléchies de scénarios d'attaque réels, à la transparence des résultats et à la richesse des informations sur les participants.

Rapports d'analystes et récompenses

Gartner

- Un Leader du Magic Quadrant de Gartner pour les plateformes de protection Endpoint dans 14 rapports consécutifs.
- 'Customers' Choice' dans les rapports Gartner® Peer Insights™ Voice of the Customer for Endpoint Protection Platforms (EPP) 2022, 2023 et 2024.

IDC

- Un Leader dans les rapports 2024 IDC MarketScape : Worldwide Modern Endpoint Security for Small and Midsize Businesses

G2

- Overall Leader | Endpoint Protection Suites : Grid Reports Spring 2023 et Fall 2023
- Overall Leader | EDR : Grid Reports Spring 2023 et Fall 2023
- Overall Leader | XDR : Fall 2023 Grid Report
- Overall Leader et solution n° 1 | XDR : Spring 2023 Grid Report

Omdia

- Overall Leader | Comprehensive Extended Detection and Response (XDR) Platforms de novembre 2022

Prix 'Tech Innovators' 2023 de CRN

- Sophos Intercept X nommé meilleure protection Endpoint

Prix 'Readers' Choice' de ChannelPro

- Sophos Intercept X remporte la médaille d'or du meilleur fournisseur de sécurité Endpoint.

Témoignages client

★★★★★

« La meilleure fonctionnalité de Sophos Endpoint Protection, c'est sa protection avancée contre les menaces. Sophos combine plusieurs technologies avancées, comme le Machine Learning, l'analyse comportementale et la détection basée sur les signatures, pour détecter et bloquer efficacement les menaces malveillantes. »

Développeur de logiciels | Secteur de la finance (non-banque) | Lire l'avis intégral sur Gartner Peer Insights

★★★★★

« Une solution tout-en-un pour les cybermenaces avancées ».

Administrateur réseau | Secteur de l'éducation | Lire l'avis intégral sur Gartner Peer Insights

★★★★★

« Mon expérience a été très satisfaisante. La solution réduit la surface d'attaque et empêche les attaques de se propager sur notre réseau d'entreprise. Avec son moteur anti-ransomware basé sur l'IA et le Machine Learning, il stopper les attaques avant qu'elles n'impactent le système, ce qui représente son plus gros avantage. »

Services TIC | Secteur de l'audiovisuel | Lire l'avis intégral sur G2

★★★★★

« Sophos est une solution extrêmement conviviale et tout aussi puissante pour les systèmes d'extrémité. »

Responsable des opérations IT | Marché intermédiaire | Lire l'avis complet sur G2

★★★★★

« Sophos Endpoint nous aide à réduire notre vulnérabilité face aux attaquants et nous assure que les systèmes de nos clients sont bien protégés contre les cybercriminels. »

Responsable Administration des systèmes, et Sauvegarde et restauration| Grande entreprise | Lire l'avis complet sur G2

Conclusion

La cybersécurité doit faire face à une multitude de menaces, qui évoluent sans cesse et rapidement. Les attaquants font constamment évoluer leurs techniques afin de contourner les défenses, et les fournisseurs de sécurité comme les entreprises n'ont pas d'autre choix que de s'adapter.

Pour y parvenir, il est primordial de faire appel à des outils de sécurité qui reposent avant tout sur un principe de prévention. Ces outils offrent des défenses automatisées et adaptatives pour bloquer et ralentir les adversaires et font gagner du temps pour mieux répondre aux attaques.

C'est pourquoi bien cerner les critères, mais aussi les résultats optimaux à atteindre dans une solution de sécurité Endpoint est essentiel, cela vous aidera à prendre une décision éclairée lors de votre choix final. Cela permettra également à votre entreprise de bénéficier de la meilleure protection possible contre les attaques actuelles.

La mission de Sophos est de protéger les entreprises et les organisations contre les menaces d'aujourd'hui et de demain. Toutes nos solutions sont conçues pour les aider à obtenir les meilleurs résultats en matière de cybersécurité. Pour en savoir plus, contactez-nous dès aujourd'hui.

Pour en savoir plus sur Sophos Endpoint et sur la protection inégalée contre les attaques avancées, rdv sur **Sophos.fr/endpoint**

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.

© 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.

2024-06-18 FR-WP (PS)

SOPHOS