SOPHOS

Guide d'achat pour la sécurité Endpoint

Plus les menaces se complexifient, plus la pression pour mettre en place une solution Endpoint adaptée augmente. Cependant, avec un marché de la sécurité saturé de solutions multiples et variées, chacune prétendant être la meilleure, il est devenu difficile de prendre une décision éclairée.

L'objet de ce guide est de vous apporter un éclairage sur les technologies clés de la sécurité Endpoint pour vous aider à mettre en place une protection adaptée à vos besoins. Et vous trouverez également les résultats de test indépendants pour vous aider à faire les bons choix parmi les différents éditeurs du marché.

Les vérités qui dérangent sur la sécurité des systèmes

La sécurité Endpoint fait beaucoup parler d'elle et il n'est pas rare de lire certaines revendications extravagantes. La réalité est que 68 % des entreprises ont été victimes d'une cyberattaque au cours de l'année passée[1]. C'est pourquoi il est fondamental que toute stratégie de sécurité se fonde sur une protection de pointe.

Mais une solution de protection à elle seule ne suffit pas. Quatre entreprises sur cinq reconnaissent manquer de personnel qualifié spécialisé sécurité[1]. Il est donc essentiel que la solution soit simple et conviviale, pour que les équipes informatiques déjà fortement sollicitées puissent tirer parti des capacités de protection. Partez du principe qu'une menace réussira à passer au travers de vos défenses alors équipez votre entreprise. Il vous faut une visibilité totale sur la manière dont elle est entrée, où elle est allée et ce qu'elle a touché, afin de neutraliser l'attaque et de combler les failles de sécurité.

Utilisez ce guide pour comprendre les technologies de protection disponibles et choisir celles qui répondent à vos besoins.

Caractéristiques et fonctions des produits

Les solutions de sécurité Endpoint, désignées sous le simple nom d'« antivirus », incluent un ensemble d'approches fondamentales (traditionnelles) et modernes (Next-Gen) pour protéger les systèmes d'extrémité. Lorsque vous évaluez des solutions, il est important de rechercher celles qui proposent un panel de techniques stoppant le plus large spectre de menaces. Il est également important de comprendre les menaces que vous souhaitez combattre.

Les menaces ciblant les systèmes Endpoint

Bien que le panorama des menaces soit en évolution constante, il existe des menaces clés ciblant les systèmes Endpoint qu'il faut prendre en considération au moment d'évaluer une solution :

- **Fichiers Portable Executable (malware) :** Lorsque l'on considère une protection Endpoint, les logiciels malveillants (ou malwares) sont les premières menaces qui nous viennent à l'esprit. Cela englobe les malwares connus, mais aussi ceux totalement inédits. Et bien souvent, les solutions peinent à détecter les malwares inconnus, ce qui est problématique quand on sait que les SophosLabs analysent près de 400 000 échantillons de malware inédits chaque jour. Les solutions devraient être capables de reconnaître les fichiers polymorphiques qui ont été modifiés pour être plus difficiles à identifier.
- **Applications potentiellement indésirables (PUA) :** Les PUA ne sont techniquement pas des malwares, mais des applications que vous ne souhaitez probablement pas avoir sur votre machine, comme les adwares. La détection des PUA est devenue très importante avec la hausse des programmes de cryptominage utilisés dans les attaques de cryptojacking.
- **Ransomwares :** Plus de la moitié des entreprises ont été ciblées par un ransomware en 2017, pour un coût moyen de 133 000 USD[2]. Les deux principaux types de ransomwares sont les chiffreurs de fichiers et les chiffreurs de disques (wipers). Les premiers, qui chiffrent les fichiers des victimes et les détiennent en échange d'une rançon, sont les plus courants. Les chiffreurs de disques verrouillent l'intégralité du lecteur de disque dur des victimes (et non pas uniquement les fichiers) ou bien les effacent complètement.
- **Attaques basées sur des exploits et attaques sans fichiers :** Toutes les attaques n'ont pas recours aux malwares. Celles basées sur un exploit utilisent des techniques utilisant des failles et des vulnérabilités des logiciels, dans le but d'accéder à votre ordinateur et de le contrôler. Les documents corrompus (typiquement un programme Microsoft Office piraté) et les scripts malveillants (un code malveillant souvent caché dans un programme ou un site Web légitime) sont des techniques couramment utilisées dans ces attaques. D'autres exemples incluent les attaques « man-in-the-browser » (utilisation d'un malware pour infecter un navigateur, permettant aux attaquants de voir et de manipuler le trafic) et le trafic malveillant (utilisant les trafics Web à des fins frauduleuses, pour contacter un serveur C&C par exemple).
- **Techniques « Active Adversary » :** De nombreuses attaques ciblant les systèmes d'extrémité se font en plusieurs étapes ou impliquent plusieurs techniques. Parmi les méthodes utilisées, nous pouvons citer l'élévation des privilèges (utilisée par les attaquants pour obtenir un accès supplémentaire à un système), le vol d'identifiants (notamment les noms et mots de passe des utilisateurs), et les Codes Cave (un code malveillant caché dans une application légitime).

Techniques modernes (Next-Gen) vs. fondamentales (traditionnelles)

Même s'ils sont commercialisés sous différentes appellations, les antivirus existent depuis de très nombreuses années et sont éprouvés face aux menaces connues. Les solutions traditionnelles s'appuient sur une variété de techniques fondamentales. Mais le panorama des menaces ayant évolué, les menaces inconnues, comme les malwares inédits, sont de plus en plus fréquentes. C'est pour cette raison que de nouvelles technologies ont vu le jour sur le marché. Les acheteurs devraient rechercher une solution offrant une combinaison entre des approches modernes, souvent appelées « Next-Gen », et des approches fondamentales. Quelques-unes des capacités clés incluent :

Capacités fondamentales :

- **Antimalware/antivirus :** Détection des malwares connus basée sur les signatures. Les moteurs antimalwares devraient pouvoir inspecter non seulement les fichiers exécutables, mais également d'autres codes, comme les fichiers JavaScript malveillants trouvés dans les sites Web.
- **Verrouillage des applications :** Prévention des comportements malveillants des applications (comme les documents Office corrompus) qui installent d'autres applications puis les exécutent.
- **Surveillance du comportement/Système de prévention des intrusions sur l'hôte (HIPS) :** Cette technologie protège les ordinateurs des virus non identifiés et des comportements suspects. Elle doit inclure l'analyse avant exécution et l'analyse comportementale runtime.
- **Protection Web :** Recherche des URL et blocage des sites Web malveillants connus. La liste des sites bloqués devrait inclure ceux exécutant des programmes en JavaScript utilisés pour le cryptominage, ainsi que les sites collectant les identifiants de connexion des utilisateurs ou toute autre donnée sensible.
- **Contrôle du Web :** Le filtrage Web permet aux administrateurs de définir les types de fichiers que les utilisateurs peuvent télécharger depuis Internet.
- **Prévention des fuites de données (DLP) :** Si un attaquant parvient à passer inaperçu, les capacités DLP sont un rempart contre l'ultime étape d'une attaque, c'est-à-dire l'exfiltration des données. La détection DLP est possible grâce au contrôle d'une multitude de types de données sensibles.

Capacités modernes :

- **Machine Learning :** Il existe plusieurs types de Machine Learning, dont le Deep Learning et ses réseaux neuronaux, les forêts d'arbres décisionnels, les analyses bayésiennes et le clustering. Indépendamment de la méthodologie utilisée, les moteurs de détection des malwares par Machine Learning devraient être conçus pour détecter les malwares connus et inconnus, sans avoir recours aux signatures. L'avantage du Machine Learning est qu'il peut détecter les malwares inédits, augmentant ainsi le taux global de détection des malwares. Au moment d'évaluer une solution basée sur le Machine Learning, les entreprises devraient considérer le taux de détection, le taux de faux positifs et les effets sur les performances.
- **Anti-exploit :** Une technologie anti-exploit est conçue pour stopper les attaquants en bloquant les outils et les techniques mis en œuvre lors de l'attaque. Par exemple, les exploits EternalBlue ou DoublePulsar ont été utilisés pour exécuter les ransomwares NotPetya et WannaCry. La technologie anti-exploit stoppe la poignée de techniques utilisées pour diffuser les malwares et réaliser des attaques, repoussant ainsi de nombreuses attaques Zero-day inédites.
- **Spécifiques aux ransomwares :** Certaines solutions sont dotées de techniques spécifiquement conçues pour empêcher le chiffrement malveillant des données par un ransomware. Souvent, les techniques spécifiques aux ransomwares permettent également la remédiation des fichiers touchés. Les solutions anti-ransomware devraient non seulement stopper les ransomwares ciblant les fichiers, mais également ceux utilisés pour effacer les disques et pour falsifier l'enregistrement d'amorçage maître.
- **Protection contre le vol d'identifiants :** Une technologie conçue pour prévenir les vols de mots de passe et des informations de hachage de la mémoire, du registre et du disque dur.

- **Protection des processus (élévation des privilèges) :** Une protection qui peut déterminer quand un jeton d'authentification est inséré dans un processus pour élever ses privilèges dans le cadre d'une attaque. Cela devrait être mis en œuvre, quelle que soit la vulnérabilité, connue ou inconnue, utilisée pour voler le jeton d'authentification.
- **Protection des processus (Code Cave) :** Elle empêche l'utilisation de techniques telles que le Code Cave et AtomBombing, fréquemment utilisées par les attaquants cherchant à profiter de la présence d'applications légitimes. Les attaquants peuvent exploiter ces appels pour forcer un processus à exécuter leur code.
- **EDR (Endpoint Detection and Response) :** Une solution EDR devrait être capable de fournir des informations détaillées pour traquer les menaces évasives, maintenir une hygiène rigoureuse des opérations de sécurité IT et analyser les incidents détectés. Il est important de prendre en considération la compatibilité entre la complexité et la convivialité d'un outil et la taille et les ressources de votre équipe. Par exemple, en choisissant une solution qui fournit des informations sur les menaces et des conseils détaillés, ce qui permet de répondre rapidement et facilement à une menace.
- **XDR (Extended Detection and Response) :** La technologie XDR va au-delà de la protection Endpoint et Serveur, en incorporant des données d'autre sources, telles que le pare-feu, la messagerie, le Cloud et les mobiles. Elle est conçue pour donner aux organisations une vue d'ensemble de leur environnement, avec la possibilité de zoomer dans les détails si nécessaire. Toutes ces informations doivent être corrélées dans un endroit centralisé, généralement appelé Data Lake, où l'utilisateur peut lancer des requêtes pour obtenir des réponses critiques pour l'entreprise.
- **Réponse aux incidents/Sécurité synchronisée :** Les solutions Endpoint devraient fournir des outils capables, au minimum, d'offrir un aperçu des événements antérieurs en vue d'éviter de futurs incidents. De manière idéale, ces solutions devraient pouvoir répondre automatiquement aux incidents, sans avoir besoin de l'intervention d'un analyste, afin d'empêcher les menaces de se propager ou de provoquer plus de dégâts. Il est important que les outils de réponse aux incidents communiquent avec les autres outils de sécurité Endpoint et les outils de sécurité réseau.
- **Managed Threat Response (MTR) :** Sophos MTR est une offre de services de recherche, de détection et de remédiation des menaces, entièrement gérée par une équipe d'experts 24 h/24 et 7 j/7. Les analystes doivent être capables de répondre aux menaces, de rechercher des indicateurs de compromission et de fournir une analyse détaillée des événements qui se sont produits, où, quand, comment et pourquoi.

La « puissance du plus » : Combiner une multitude de techniques pour une sécurité Endpoint complète

Au moment d'évaluer une solution Endpoint, les entreprises ne devraient pas s'intéresser qu'à une seule fonction primaire. Au contraire, elles devraient rechercher tout en ensemble de fonctions innovantes qui englobent des techniques modernes, comme le Machine Learning, des approches fondamentales éprouvées, ainsi que la fonctionnalité 'Endpoint detection and response' (EDR) pour l'investigation et la réponse aux incidents. Compter sur une seule fonction dominante, même s'il s'agit d'une technique de pointe, signifie que vous serez vulnérable en d'autres points. Inversement, une approche de défense en profondeur, dotée de nombreuses couches solides de protection, arrêtera un éventail de menaces plus large. C'est ce que nous appelons la « puissance du plus », c'est-à-dire une combinaison de techniques fondamentales, 'plus' le Machine Learning, 'plus' un anti-exploit, 'plus' un anti-ransomware, 'plus' l'EDR, 'plus'...

Lors de votre évaluation, demandez aux différents éditeurs la liste des techniques incluses dans leurs solutions. Chaque composant est-il robuste ? Quelles menaces sont-ils capables d'arrêter ? Se reposent-ils uniquement sur une technique principale ? Que se passe-t-il si celle-ci échoue ?

Sophos face à la concurrence

Comparer différents produits dotés de différentes fonctionnalités est une tâche assez ardue, mais comparer leurs performances lors de simulations d'attaques, où les actions des attaquants sont potentiellement infinies et imprévisibles, est une tâche quasiment impossible. Pour ceux qui préfèrent évaluer eux-mêmes les produits, un guide d'introduction aux évaluations est disponible ici. Cependant, de nombreuses organisations font confiance aux tests réalisés par des cabinets indépendants pour choisir leurs solutions.

Évaluation et certification à 360 degrés

Dans le test Endpoint de MRG Effitas au quatrième trimestre 2020, Sophos Intercept X a bloqué 100 % des attaques testées. En plus de Sophos Intercept X, Bitdefender Endpoint Security et Malwarebytes Endpoint Protection ont reçu la note la plus élevée (Level 1). ESET Endpoint Security, F-Secure Computer Protection Premium and Microsoft Windows Defender ont obtenu le Level 2.

TEST UTILISÉ	RÉSULTATS DE SOPHOS
Test 'In the Wild 360'/spectre complet	Taux de blocage de 100 %
Malwares financiers	Taux de blocage de 100 %
Ransomwares	Taux de blocage de 100 %
Test PUA/Adware	Taux de blocage de 100 %
Test exploit/sans fichier	Taux de blocage de 100 %
Test de faux positif	0 faux positif

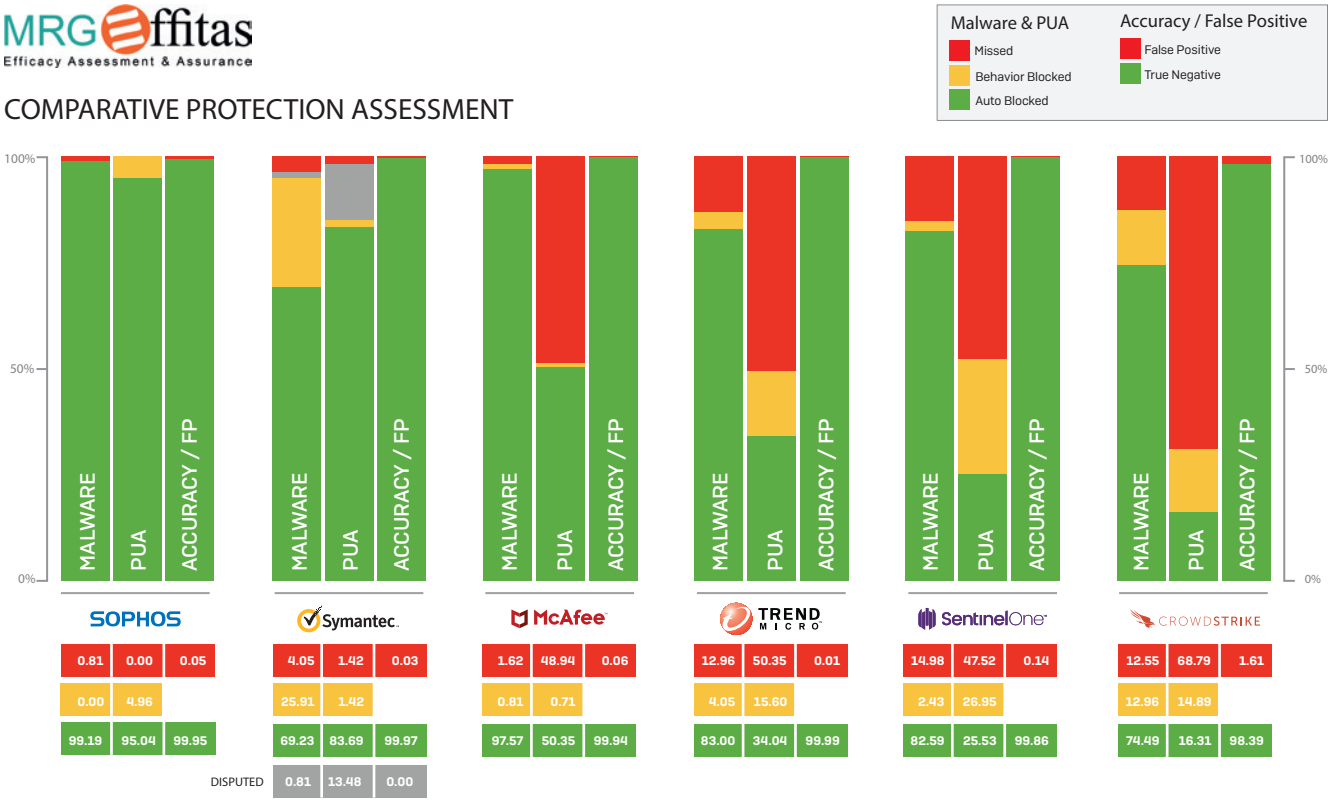
Avast Business Antivirus, Avira Antivirus Pro, Symantec Endpoint Protection et Trend Micro Security ont tous échoué au test. Consultez le rapport complet ici.

Test de protection antimalware par MRG Effitas

MRG Effitas a passé au crible plusieurs produits Endpoint concurrents par une série de tests afin de comparer leurs capacités à détecter les malwares et les applications potentiellement indésirables (PUA). Six éditeurs différents, dont Sophos, ont été choisis pour y participer. Sophos s'est classé premier pour la détection des malwares et premier pour la détection des PUA. Sophos a également obtenu des résultats impressionnants au test des faux positifs.

MRG Effitas
Efficacy Assessment & Assurance

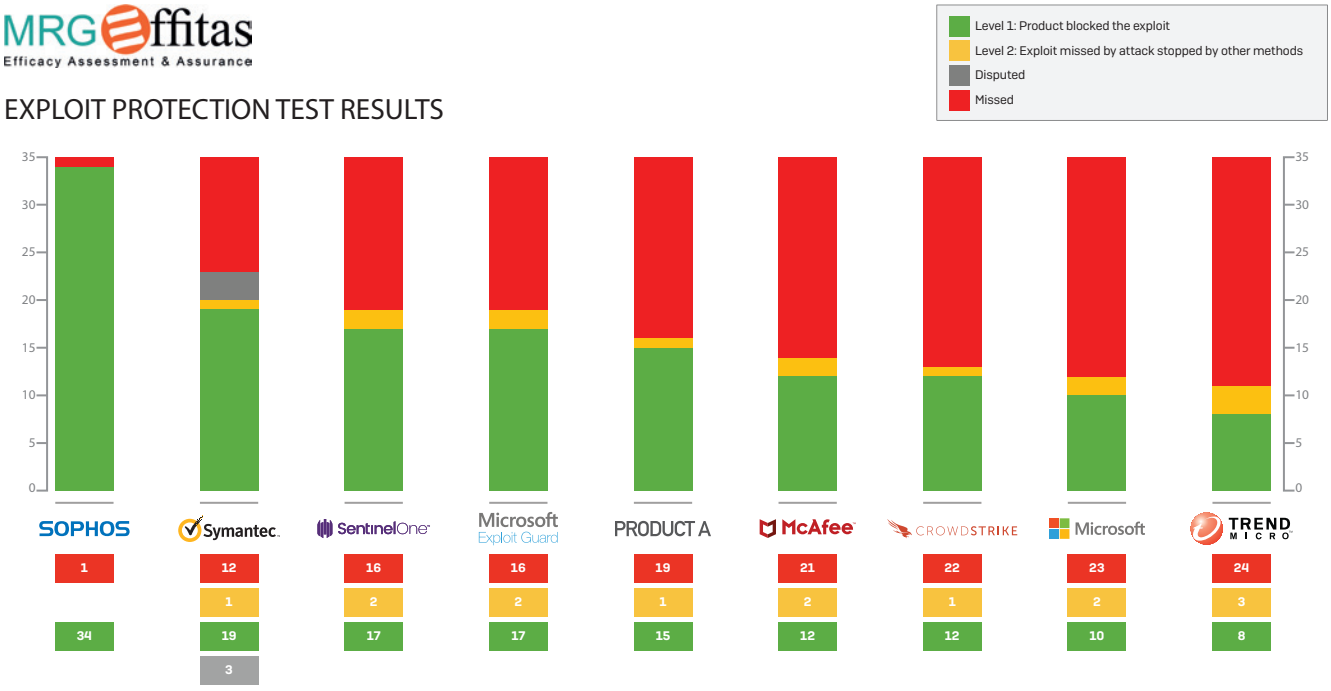
COMPARATIVE PROTECTION ASSESSMENT



Consultez les résultats complets ici.

Test de protection anti-exploit et post-exploit par MRG Effitas

Pour faire suite à son test de protection antimalware, MRG Effitas a également publié un rapport comparant les performances de différentes solutions Endpoint à stopper les techniques spécifiques aux exploits. Sophos Intercept X a largement surpassé les autres solutions testées. Sophos a en effet été capable de bloquer deux fois plus de techniques d'exploit que les autres outils testés.



Obtenez l'intégralité du rapport ici.

Rapport des SE Labs sur les protections Endpoint

Sophos Intercept X Advanced a obtenu un score de 100 % de performances globales pour la protection Endpoint des grandes et des petites entreprises dans le rapport de test de SE Labs pour la protection Endpoint (Jan-Mar 2020). SE Labs a systématiquement attribué la note AAA à Intercept X Advanced dans chacun des tests effectués depuis avril 2018.

TAUX DE PRÉCISION TOTALE			
Produits	*Taux de précision totale*	*Précision totale (%)*	*Récompense*
Sophos Intercept X Advanced	1 136	100 %	AAA
ESET Endpoint Security	1 136	100 %	AAA
Kaspersky Small Office Security	1 136	100 %	AAA
Symantec Endpoint Protection Cloud	1 117	98 %	AAA
Trend Micro Worry-Free Security Services	1 114	98%	AAA
McAfee Endpoint Security	1 107	97%	AAA
Microsoft Windows Defender Enterprise	1 101	97%	AAA
Bitdefender GravityZone Endpoint Security	1 099,5	97%	AAA
Webroot SecureAnywhere Endpoint Protection	993	87%	A

Source : SE Labs Small Business Protection Jan-Mar 2020

TAUX DE PRÉCISION TOTALE			
Produits	*Taux de précision totale*	*Précision totale (%)*	*Récompense*
Sophos Intercept X Advanced	1 136	100 %	AAA
ESET Endpoint Security	1 136	100 %	AAA
Kaspersky Small Office Security	1 136	100 %	AAA
Symantec Endpoint Protection Cloud	1 117	98 %	AAA
McAfee Endpoint Security	1 107	97%	AAA
Microsoft Windows Defender Enterprise	1 101	97%	AAA
Bitdefender GravityZone Endpoint Security	1 099,5	97%	AAA
Crowdstrike Falcon	1 089	96%	AAA
VIPRE Endpoint Security	1 087	96%	AAA
FireEye Endpoint Security	1 052	93%	AA

Source : SE Labs Small Business Protection Jan-Mar 2020

Magic Quadrant de Gartner pour les plateformes de protection Endpoint

Source: Gartner (August 2019)

Le Magic Quadrant de Gartner pour les plateformes de protection Endpoint est un outil d'analyse qui évalue les éditeurs en fonction de leur vision globale et de leur capacité à l'exécuter. Sophos se positionne comme « Leader », pour la douzième fois consécutive. Gartner a félicité Sophos pour sa protection Endpoint robuste, en mentionnant la confiance des clients dans les défenses anti-ransomware éprouvées dont la fonction de restauration des fichiers chiffrés, les capacités EDR (Endpoint Detection and Response) étendues pour la traque des menaces et les opérations informatiques, ainsi que la gestion centralisée de toutes les solutions Sophos dans Sophos Central.

The Forrester Wave™: Endpoint Security Suites

Les analystes de Forrester Research, Inc. réalisent des évaluations produit approfondies pour créer leurs rapports et s'entretiennent dans ce but avec les éditeurs et leurs clients. Ils évaluent les éditeurs en fonction de la robustesse de leur produit et de leur stratégie. Sophos a une fois de plus été nommé « Leader » dans le rapport Forrester Wave for Endpoint Protection Suites.

Obtenez l'intégralité du rapport ici.

Avis de SC Magazine :

SC Magazine a donné à Intercept X une note parfaite, le décrivant comme :

« ...une solution de sécurité endpoint digne de ce nom, facile à installer, qui ajoute de l'expertise en fournissant des informations contextuelles enrichies sans augmenter les effectifs de l'équipe de sécurité. »

Lisez l'article complet ici.

AV-Comparatives

Intercept X est apparu pour la première fois dans le Business Security Test d'AV-Comparatives où il a été classé n° 1 pour la détection des malwares. Nous avons obtenu un taux de détection de 99,7 % avec seulement une fausse alarme dans le test « Real-World Protection » et un taux de 99,9 % et aucune fausse alarme dans le test « Malware Protection ».

	TAUX DE PROTECTION ANTI-MALWARE	FAUSSES ALARMES AVEC UN LOGICIEL PROFESSIONNEL COURANT
Avast, Bitdefender, Panda, Sophos, SparkCognition	99,9 %	0
Cisco, Symantec, Trend Micro	99,8 %	0
K7, McAfee	99,7 %	0
Seqrite	99,6%	0
FireEye, Microsoft	99,5%	0
CrowdStrike, Endgame, VIPRE	99,2%	0
Kaspersky Lab	99,0 %	0
Fortinet	98,9 %	0
ESET	99,5 %	0

Source : AV-Comparatives Business Security Test Jan-Mar 2020

PC Magazine

Pour PC Magazine, Intercept X est « une excellente solution de défense contre les logiciels malveillants pour les entreprises de toutes tailles ». La rédaction ajoute qu'elle offre « d'excellentes fonctionnalités de détection et anti-exploit », « des fonctionnalités EDR (Endpoint Detection and Response) entièrement intégrées » et « un excellent contrôle des politiques de sécurité ».

Source : https://uk.pcmag.com/software/121154/sophos-intercept-x-endpoint-protection

AV-Test (Mac)

Sophos a obtenu un score de 6/6 pour sa protection, 6/6 pour sa performance et 6/6 pour son utilisation.

Source : https://www.av-test.org/en/antivirus/business-macos/macos-catalina/june-2020/sophos-endpoint-9.9-202105/

Intercept X : résultats de tests indépendants et principaux rapports d'analystes

SE Labs

- Note AAA pour les grandes entreprises – 100 % de performances globales
- Note AAA pour les PME – 100 % de performances globales
- Note AAA pour les particuliers – 100 % de performances globales

AV-Comparatives

- Classé nº 1 pour l'identification des malwares (99,9 % de détection, zéro fausse alarme)

MRG Effitas

- Classé nº 1 pour la protection anti-malware
- Classé nº°1 pour la protection anti-exploit
- Taux de blocage de 100 %, 0 faux positif — Évaluation à 360 degrés

PC Magazine

- Choix de la rédaction

AV-Test

- AV-Test (macOS) : Score parfait
- AV-Test (Android) : Score parfait

Gartner

- Leader : 2020 EPP Magic Quadrant

Forrester

- Leader : 2019 Endpoint Security Wave

IDC

- Leader : 2019-2020 Enterprise Mobility Management Marketscape
- Leader : 2020 Worldwide Mobile Threat Management Marketscape

Renforcer votre sécurité : Envisagez une solution de protection complète

Une solution de sécurité Endpoint est un des éléments d'une stratégie de sécurité globale. Les entreprises d'aujourd'hui doivent envisager la protection de l'ensemble de l'environnement informatique et non pas uniquement des systèmes d'extrémité.

Idéalement, un éditeur devrait à lui seul proposer des solutions fonctionnant en synergie pour garantir la protection et la mise en application des politiques homogènes au sein de votre organisation. Le fait de travailler avec un seul éditeur permet d'obtenir une meilleure sécurité, de réduire la charge administrative et d'alléger les coûts.

Certaines technologies spécifiques sont à envisager en complément d'une protection Endpoint. C'est le cas du chiffrement intégral du disque (FDE), de la gestion des appareils mobiles (MDM), de la sécurité des mobiles, d'une passerelle de messagerie sécurisée, d'une protection spécialisée pour les serveurs ou les machines virtuelles et de la sécurité synchronisée entre les postes et le réseau.

Renforcer votre sécurité : Endpoint Detection and Response

Sophos Intercept X Advanced est la première solution EDR conçue pour les administrateurs IT et les analystes de sécurité pour les aider à résoudre les opérations informatiques et traquer les menaces. Il vous permet de poser n'importe quelle question sur un événement passé ou en cours survenant sur vos postes. Traquez les menaces pour détecter les adversaires actifs, ou exploitez les opérations informatiques pour maintenir l'hygiène de la sécurité informatique Lorsqu'un problème est détecté, répondez à distance avec précision.

Posez des questions précises sur la traque des menaces et les opérations IT, telles que :

- Des processus tentent-ils d'établir une connexion réseau sur des ports non standards ?
- Quels appareils ont des vulnérabilités connues, des services inconnus ou des extensions de navigateur non autorisées ?
- Comprendre la portée et l'impact des incidents de sécurité.
- Détecter les attaques qui peuvent passer inaperçues.
- Rechercher des indicateurs de mise en danger du réseau.
- Prioriser les événements pour permettre une investigation plus poussée.
- Analyser les fichiers pour déterminer s'ils constituent une menace ou une PUA.
- Rendre compte en toute confiance de la posture de sécurité de l'entreprise, et ce à tout moment.

Niveau supérieur de visibilité : Extended Detection and Response

Allez au-delà des postes et des serveurs, en corrélant les données du pare-feu, de la messagerie et d'autres sources*. Sophos XDR fournit une vue d'ensemble de la posture de cybersécurité de votre organisation, avec la possibilité de zoomer dans les détails selon vos besoins.

Posez vos questions et obtenez des réponses, notamment :

- Pourquoi la connexion au réseau du bureau est-elle lente ?
- Y a-t-il des appareils non gérés ou non protégés dans mon parc ?
- Prolonger l'investigation jusqu'à 30 jours sans remettre un appareil en ligne
- Utiliser les détections ATP et IPS du pare-feu pour analyser les hôtes et les appareils suspects
- Comparer les informations de l'en-tête de l'email avec d'autres indicateurs de compromission
- Revenir 30 jours en arrière pour détecter toute activité inhabituelle sur un appareil disparu ou détruit

Les avantages de Sophos Intercept X incluent :

- L'EDR associée à la meilleure protection Endpoint
- Le XDR qui inclut le pare-feu, la messagerie et d'autres sources de données pour offrir une image complète de votre environnement.
- Des requêtes SQL avancées et pré-écrites pour obtenir les informations dont vous avez besoin
- L'analyse des malwares par Deep Learning afin de reproduire le travail des analystes
- Intelligence des SophosLabs sur les menaces, à la demande
- Détection et hiérarchisation des événements suspects par Machine Learning
- Investigations guidées pour un EDR accessible mais puissant
- Réponse aux incidents en un seul clic
- Service assuré par des experts 24/7 : Managed Threat Response

Service assuré par des experts 24/7 : Managed Threat Response

Sophos MTR (Managed Threat Response) assiste votre entreprise avec une équipe d'experts de haut niveau spécialisés dans la traque et la remédiation des menaces, qui prend les mesures nécessaires en votre nom pour neutraliser les menaces, même les plus sophistiquées. Avantages principaux :

- Traque des menaces à partir d'indices 24 h/24 7j/7
- Diagnostic de sécurité
- Rapport d'activité
- Assistance téléphonique directe et un interlocuteur dédié
- Protection avancée contre les menaces les plus récentes avec Intercept X

FONCTIONNALITÉS	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH EDR	INTERCEPT X ADVANCED WITH XDR	INTERCEPT X ADVANCED WITH MTR STANDARD	INTERCEPT X ADVANCED WITH MTR ADVANCED
Protections fondamentales (dont contrôle des applications, détection du comportement, etc.)	✓	✓	✓	✓	✓
Protection Next-Gen (dont Deep Learning, anti-ransomware, protection contre les attaques sans fichiers, etc.)	✓	✓	✓	✓	✓
EDR (Endpoint Detection and Response)		✓	✓	✓	✓
XDR (Extended detection and response)				Voir note ✓	Voir note ✓
Managed Threat Response (MTR – service 24/7/365 de Threat Hunting et de réponse aux menaces)					✓
MTR Advanced (Traque sans indices de départ, interlocuteur dédié, etc.)					

Remarque : L'équipe MTR pourra exploiter les données et la fonctionnalité XDR pour les clients MTR Advanced. Toutefois, les clients MTR seront limités à la fonctionnalité EDR dans leur console Sophos Central, à moins qu'ils n'achètent une licence XDR.

Évaluer la sécurité Endpoint : Les 10 questions à poser

Pour évaluer une solution de protection Endpoint, commencez par poser à l'éditeur les questions suivantes :

1. Le produit se base-t-il sur des techniques fondamentales, modernes ou les deux ? Quelles sont les fonctions spécifiques au cœur de la technologie ?
2. Comment le produit détecte-t-il les menaces inconnues ? Utilise-t-il le Machine Learning ?
3. Pour les produits déclarant exploiter le Machine Learning, quel type de Machine Learning est-il utilisé ? D'où proviennent les données d'apprentissage ? Depuis combien de temps le modèle a-t-il été en production ?
4. Existe-t-il une technologie pour prévenir les attaques basées sur les exploits et les attaques sans fichiers ? Quelles techniques anti-exploit sont utilisées, et quels types d'attaques peuvent-elles détecter ?
5. Le produit est-il doté d'une technologie spécifiquement conçue pour stopper les ransomwares ?
6. L'éditeur peut-il fournir les résultats de tests indépendants validant son approche ?
7. Le produit peut-il poser des questions précises sur la traque des menaces et les opérations IT ? Quelle est la durée de conservation des données pour les requêtes ?
8. Quelle niveau de visibilité sur une attaque l'éditeur fournit-il, telle que l'analyse détaillée des attaques (RCA) ?
9. Le produit répond-il automatiquement aux menaces ? Peut-il automatiquement nettoyer une menace et répondre à un incident ?
10. Le produit peut-il vous permettre d'accéder à distance aux appareils pour effectuer des analyses complémentaires et prendre les mesures nécessaires ?

Conclusion

La complexité et le nombre de cybermenaces ne cessent de croître, et il est plus que jamais vital de protéger efficacement ses systèmes Endpoint. Comprendre les menaces et les différentes technologies de sécurité disponibles vous permettra de choisir une sécurité Endpoint en toute connaissance et dotera votre entreprise de la meilleure protection possible contre les attaques d'aujourd'hui.

Source :

1 Sept vérités qui dérangent sur la sécurité des systèmes, mars 2019. Une enquête indépendante réalisée pour Sophos auprès de 3 100 responsables informatiques dans 12 pays différents.

2 Enquête sur la sécurité Endpoint, 2018

3 MRG Effitas Comparative Malware Protection Assessment, février 2018

Gartner Magic Quadrant for Endpoint Protection Platforms, Ian McShane, Eric Ouellet, Avivah Litan, Prateek Bhajanka, 24 janvier 2018. Gartner dégage toute responsabilité vis-à-vis des fabricants, produits ou services décrits dans ses publications et ne recommande pas aux utilisateurs de sélectionner exclusivement les fabricants classés dans son Magic Quadrant. 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.

The Forrester Wave™ : Endpoint Security Suites, Q3 2019, par Chris Sherman avec Stephanie Balaouras, Merritt Maxim, Matthew Flug et Peggy Dostie, 23 septembre 2019

Essayez-le gratuitement

Inscrivez-vous à une évaluation gratuite de 30 jours sur sophos.fr/intercept-x

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

2021-03-21 FR(MP)

SOPHOS