SOPHOS
Security made simple.

Guide d'achat pour la sécurité des systèmes d'extrémité

Il peut sembler difficile d'évaluer les composants requis en matière de protection des systèmes d'extrémité. Grâce aux résultats des recherches et des tests indépendants contenus dans ce guide, vous serez à même d'évaluer vos besoins et de choisir le produit adapté.

Il faut plus qu'un simple antivirus pour bloquer les menaces modernes. La protection des actifs de l'entreprise passe par une stratégie informatique robuste, composée entre autres d'une solution performante pour la protection des systèmes d'extrémité. Votre solution devrait être capable de prévenir, de détecter et de résoudre toutes les attaques de malwares et autres menaces avancées. Elle devrait également inclure des fonctions telles que le filtrage du Web et le contrôle des périphériques, qui vous permettent d'appliquer une politique de sécurité homogène dans toute votre entreprise. Afin de gagner du temps et des ressources, et d'assurer une protection durable, il est conseillé de choisir une solution évolutive, facile à installer et à administrer.

Nous examinerons les principaux fournisseurs du marché en fonction de leur part de marché et de l'analyse des spécialistes : Sophos, Kaspersky Lab, Intel Security (McAfee), Symantec et Trend Micro. Chaque solution sera évaluée selon les critères suivants :

- Product Features and Capabilities
- Évaluations des analystes du marché
- Résultats des tests indépendants
- L'avis des clients

Nous apporterons également d'autres informations supplémentaires qui vous aideront à choisir la meilleure solution pour protéger efficacement les systèmes d'extrémité de votre entreprise.

- Comment renforcer votre sécurité : envisagez une solution de protection complète
- Évaluation de la protection des systèmes d'extrémité : questions à poser

Caractéristiques et fonctions produit

Les solutions de sécurité de base pour les systèmes d'extrémité comprennent habituellement des fonctions antivirus, antimalware et antispyware. Mais selon les analystes de l'industrie, les entreprises ont besoin de plus que ces simples fonctions pour être protégées contre les menaces avancées actuelles et prévenir les pertes de données. Des fonctionnalités telles que la détection du trafic malveillant, le contrôle des périphériques, le contrôle des applications, le filtrage de la productivité du Web ou encore la prévention des pertes de données peuvent les y aider. Même si ces fonctionnalités ne vous sont pas essentielles aujourd'hui, il est possible qu'elles le deviennent à l'avenir étant donné la complexité croissante des menaces.

En outre , les entreprise devront tenir compte des fonctions d'administration disponibles destinées à rendre le produit simple du point de vue du déploiement, de la configuration et de la maintenance.

Le tableau suivant dresse la liste des fonctionnalités disponibles dans les solutions de protection des systèmes d'extrémité gérées de manière centralisée de chaque fournisseur :

	Sophos	Intel Security (McAfee)	Kaspersky Lab	Symantec	Trend Micro
Administration locale	✔	✔	✔	✔	✔
Administration basée dans le Cloud (SaaS)	✔	✔	✗	✔	✔
Politiques basées sur les périphériques	✔	✔	✔	✔	✔
Politiques basées sur les utilisateurs	✔	✔	Limitées	✔	✗
Contrôle des périphériques	✔	✔	✔	✔	✔
Prévention des fuites de données (DLP)	✔	✔	✗	✔	✔
Contrôle des applications	✔	✔	✔	✔	✗
Filtrage du Web par catégorie	✔	✔	✔	✔	✔
Détection du trafic malveillant	✔	✔	✗	✗	✔
Synchronisation à Active Directory	✔	✔	Importation uniquement	✔	✔
Sécurité synchronisée (Endpoint + réseau)	✔	Composant additionnel	✗	✗	✗

Évaluations des analystes du marché

Les analystes du secteur, tels que Gartner et Info-Tech Research Group, sont des sociétés indépendantes qui évaluent et notent les fournisseurs de technologies au nom de leurs entreprises clientes. Leurs rapports annuels, comme ceux mentionnés ci-dessous, fournissent des informations impartiales pour aider les organisations à prendre des décisions d'achat éclairées.

	Sophos	Intel Security (McAfee)	Kaspersky Lab	Symantec	Trend Micro
Quadrant magique de Gartner pour les plates-formes de protection Endpoint	Leader	Leader	Leader	Leader	Leader
Panorama Info-Tech des fournisseurs de protection des systèmes d'extrémité	Champion et meilleure note globale	Market Pillar	Innovator	Market Pillar	Champion

Quadrant magique de Gartner pour les plates-formes de protection Endpoint

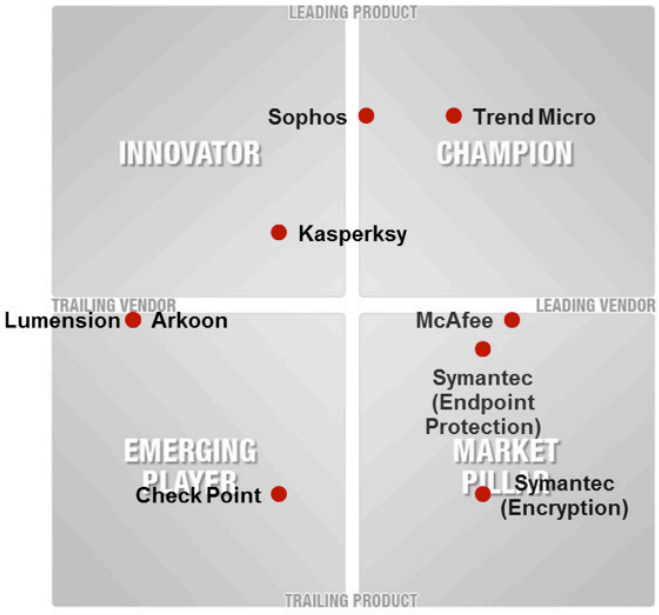
Le Quadrant Magique pour les « Endpoint Protection Platforms » de Gartner est un outil de recherche qui évalue les éditeurs en fonction de l'exhaustivité de leur vision et de la qualité de leur exécution. En 2014, 18 éditeurs différents sont passés au crible. Sophos, Kaspersky Lab, Intel Security (McAfee), Symantec et Trend Micro sont arrivés en tête du Quadrant des Leaders. Sophos est Leader pour la huitième année consécutive.

Quadrant magique pour les plateformes Endpoint Protection par Peter Firstbrook, John Girard, Neil MacDonald, le 22 Décembre, 2014

Déclaration de non-responsabilité : 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 le quadrant des leaders. 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.

Panorama des fournisseurs de protection des systèmes d'extrémité Info-Tech

Dans son rapport, Info-Tech Research Group effectue des tests d'évaluation des différents éditeurs basés sur la qualité du produit et ses atouts pour les entreprises. Le rapport stipule que les "Champions reçoivent des scores élevés pour la plupart des critères d'évaluation et offrent une excellente prestation. Ils ont une forte présence sur le marché et sont généralement les créateurs de tendances pour le secteur." Sophos est l'un des deux seuls champions dans du rapport 2014. Info-Tech a également donné à Sophos la meilleure note globale.



Résultats des tests indépendants

Des tests indépendants, comme ceux présentés ci-dessous, comparent les taux de détection, les taux de faux positifs et les performances (effet sur la vitesse du système) dans un environnement de laboratoire contrôlé. Les conditions de laboratoire, cependant, ne reflètent pas toujours la protection et les performances en conditions réelles. Il convient donc de tenir compte des fonctions de prévention, de détection et de résolution disponibles dans chaque solution.

		Sophos	Intel Security (McAfee)	Kaspersky Lab	Symantec	Trend Micro
AV-Test Business Windows Client Mai-juillet 2015	**Scores de protection**	6.0/6.0	6.0/6.0	6.0/6.0	6.0/6.0	6.0/6.0
Dennis Technology Labs Small Business Anti-Virus Protection Jan-Mars 2015	**Récompense**	AAA	A	AAA	AAA	B
	Précision totale	94%	84%	100%	100%	73%
Test de performances AV-Comparatives Mai 2015		Advanced+ ★★★	Advanced+ ★★★	Advanced+ ★★★	Non testé	Advanced ★★

L'avis des clients

Parfois, la meilleure façon d'évaluer un fournisseur est de demander directement aux clients ce qu'ils en pensent. C'est exactement ce que fait Spiceworks en demandant l'avis en ligne de sa communauté, soit six millions de professionnels de l'informatique. Voici les résultats pour les principaux fournisseurs de sécurité des systèmes d'extrémité :

	Sophos	Intel Security (McAfee)	Kaspersky Lab	Symantec	Trend Micro
Note moyenne (maximum de 5 étoiles)	★★★★½	★★	★★★★	★★½	★★★½

En outre, le site Information Security™ magazine and SearchSecurity.com a demandé à plus de 1 700 cadres et responsables de la sécurité informatique d'évaluer leurs produits préférés dans 22 catégories. Sophos est l'un des deux gagnants des Readers' Choice Awards 2014 dans la catégorie Sécurité des systèmes d'extrémité.

Comment renforcer votre sécurité : envisagez une solution de protection complète

Une solution de sécurité des systèmes d'extrémité protège vos ordinateurs contre les logiciels malveillants et vous aide à appliquer votre politique de sécurité sur ces ordinateurs. Ce n'est toutefois qu'un seul élément d'une stratégie de sécurité globale. Les organisations d'aujourd'hui ont raison d'envisager la protection de l'environnement des utilisateurs dans son ensemble et non plus seulement les systèmes d'extrémité. Idéalement, un seul fournisseur devrait proposer un ensemble de solutions qui fonctionnent en synergie pour garantir une protection et une mise en application des politiques homogènes dans votre organisation. Le fait de travailler avec un seul fournisseur permet d'obtenir une meilleure sécurité, de réduire la charge administrative et d'alléger les coûts.

Voici certaines technologies spécifiques à envisager en plus de la protection des systèmes d'extrémité

- Chiffrement intégral du disque
- Gestion des mobiles (Mobile device management, MDM)
- Sécurité des mobiles (antivirus)
- Sécurisation des passerelles de messagerie (antispam, antimalware, chiffrement)
- Sécurisation des passerelles Web (filtrage du contenu, antimalware, édition de rapports)
- Protection de machines virtuelles ou serveur spécialisé
- Sécurité synchronisée - Protections Endpoint et réseau travaillent ensemble pour aider à la prise de décisions

Évaluation de la protection des systèmes d'extrémité : questions à poser

Les solutions pour les systèmes d'extrémité se targuent d'offrir de nombreuses fonctionnalités différentes. Pour évaluer un produit spécifique, vous pouvez commencer par poser au fournisseur les questions suivantes :

1. En quoi consiste exactement le déploiement et la configuration de la solution pour obtenir une protection optimale ou qui suit les « meilleures pratiques » ?
2. Quelles mesures sont nécessaires pour ajouter des exceptions aux politiques (par exemple, permettre l'accès à un lecteur USB ou à un site Web spécifiques) ?
3. Quel impact (sur les performances et la convivialité) le produit aura-t-il sur les utilisateurs finaux ?
4. Quel niveau de support et quels horaires sont proposés en standard avec le produit ?
5. Comment le produit a-t-il évolué récemment pour protéger contre les nouvelles menaces avancées ?
6. Le produit fournit-il un filtrage et une protection Web et ce, même lorsque les utilisateurs sont hors du réseau de l'entreprise ?
7. Quelles offres groupées ou suites sont disponibles pour étendre les capacités du produit et protéger davantage les utilisateurs et les données ?
8. Comment votre fournisseur vous permet-il d'étendre les fonctionnalités de votre protection Endpoint en les intégrant à votre sécurité réseau ?

Équipe commerciale France
Tél. : 01 34 34 80 00
E-mail : info@sophos.fr

2015-10 BG-FR (NP)