# Protection antivirus pour les entreprises

## AVRIL – JUIN 2013

Dennis Technology Labs
www.DennisTechnologyLabs.com

Ce rapport vise à comparer l'efficacité des solutions anti-malwares proposées par des sociétés de sécurité renommées.

Pour ce faire, les solutions ont été exposées à des cyber-menaces pendant la période du test. Cette exposition a été effectuée en conditions réelles, afin de refléter au mieux l'expérience client.

Les résultats reflètent ce qui se serait passé si un utilisateur avait utilisé l'une des solutions et visité un site Web infecté.

## INTRODUCTION

- **Solutions testées**
  - Kaspersky Endpoint Security for Windows
  - McAfee VirusScan, HIPs et SiteAdvisor
  - Microsoft System Center Endpoint Protection
  - Symantec Endpoint Protection
  - Trend Micro OfficeScan et Intrusion Defense Firewall

- **L'efficacité des solutions anti-malwares est très variable.**
  Bien que chaque solution ait été mise en péril au moins une fois, la plus efficace a protégé le système dans la grande majorité des cas. Les meilleures solutions (de Kaspersky et Symantec) ont affiché une efficacité de 98-99 %. Cependant, la solution la moins efficace (Microsoft System Center Endpoint Protection) a été mise en péril par 18 % des menaces.

- **L'une des approches efficaces est de bloquer les sites qui ont la réputation d'être malveillants.**
  Les solutions qui ont averti les utilisateurs de leur visite sur un site malveillant dès le début ont obtenu un avantage significatif. Si le logiciel malveillant ne parvient pas à se télécharger sur l'ordinateur de la victime, cela ne représente pas de défi pour la solution anti-malwares.

- **Les solutions anti-malwares ont globalement montré une grande précision dans leur évaluation des logiciels authentiques.**
  Les faux positifs ont été rares au cours de ce test. Bien que la plupart des solutions en aient généré au moins un, ils ont été très peu nombreux. La solution de Trend Micro a été la moins précise sur cet aspect.

- **Quelle a été la meilleure solution ?**
  Le programme le plus précis a été Kaspersky Endpoint Security for Windows, suivi de très près par Symantec Endpoint Protection. Les deux solutions ont reçu le prix AAA. Aucune autre solution testée n'a reçu de prix.

Simon Edwards, Dennis Technology Labs, 5 juillet 2013

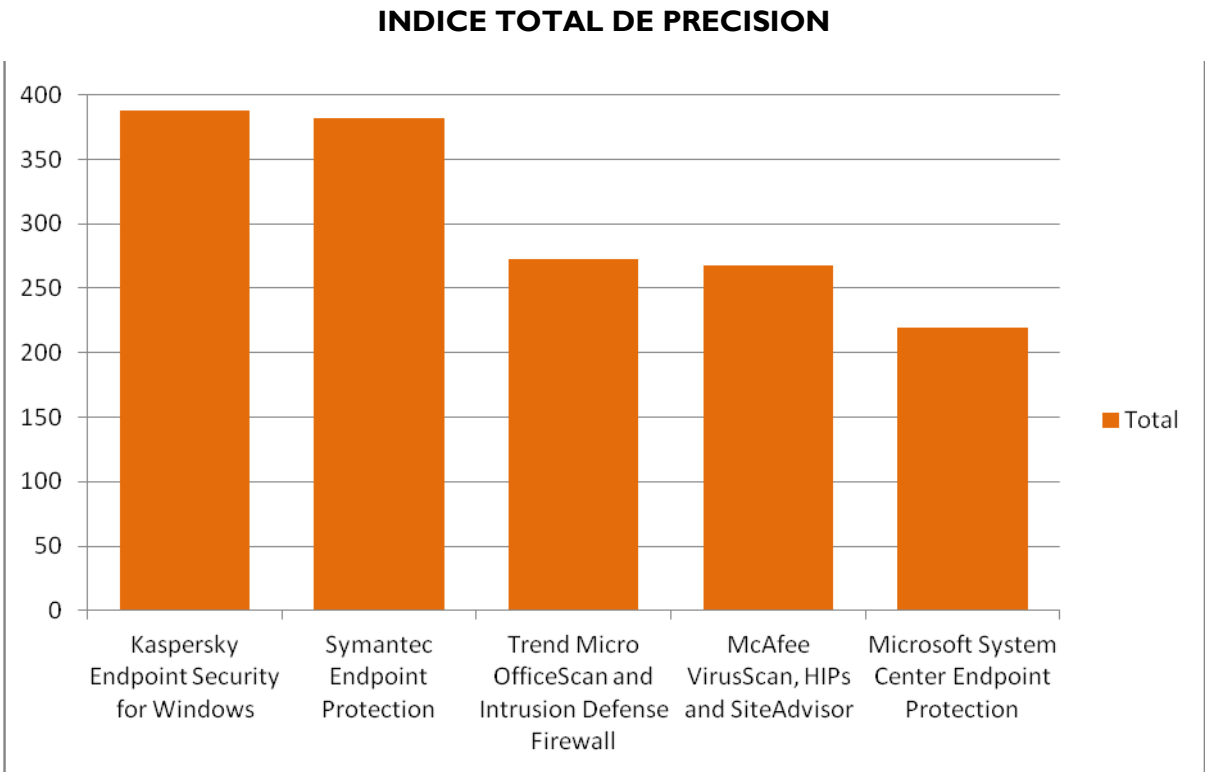
# TABLE DES MATIERES

## 1. INDICE TOTAL DE PRECISION

L'indice total de précision a permis de mesurer l'efficacité des solutions de sécurité et de présenter les résultats sur un seul graphique.

Les solutions anti-malwares ne sont pas simplement censées détecter les menaces. Elles doivent aussi permettre aux logiciels authentiques de fonctionner sans accroc.

Les résultats ci-dessous prennent en compte le degré d'efficacité des solutions dans leur gestion des menaces et des logiciels authentiques.




**L'indice total de précision prend en compte les succès et les échecs des solutions face à des applications à la fois authentiques et malveillantes.**

Nous avons donc effectué deux tests différents : l'un a mesuré la réaction des solutions face aux cybermenaces, l'autre a mesuré la manière dont ils ont géré les programmes authentiques.

La solution idéale doit bloquer toutes les menaces, tout en permettant aux applications authentiques de fonctionner normalement.

Lorsqu'une solution ne parvient pas à protéger le système contre une menace, il est en péril. Lorsqu'elle avertit, ou même bloque, un logiciel authentique, elle génère alors un résultat appelé « faux positif ».

Les solutions ont gagné des points lorsqu'elles ont réussi à bloquer une menace, tout en permettant aux utilisateurs d'installer et d'utiliser des logiciels authentiques. À l'inverse, elles ont perdu des points lorsqu'elles n'ont pas réussi à bloquer la menace, ou qu'elles n'ont pas géré correctement des fichiers authentiques.

Chaque solution s'est alors vue attribuer une note finale, moyenne de sa performance dans les deux tests, « menace » et « logiciel authentique ».

Ces résultats représentent l'indice de précision combiné en prenant en compte la performance de chaque solution avec les menaces et les logiciels non malveillants.

L'indice maximal possible est de 400, et l'indice minimal de -1 000.

Voir *5. Faux positifs* en page 9 pour consulter les résultats détaillés ainsi qu'une explication de la méthode de calcul des indices de faux positifs.

INDICE TOTAL DE PRÉCISION

| Produit | Indice total de précision | Pourcentage | Prix |
|---|---|---|---|
| Kaspersky Endpoint Security for Windows | 388 | 97% | AAA. |
| Symantec Endpoint Protection | 382 | 96% | AAA. |
| Trend Micro OfficeScan et Intrusion Defense Firewall | 272.4 | 68% | - |
| McAfee VirusScan, HIPs et SiteAdvisor | 267.9 | 67% | - |
| Microsoft System Center Endpoint Protection | 219 | 55% | - |

- **Prix**

Les solutions suivantes ont remporté le prix Dennis Technology Labs :


Kaspersky Endpoint Security for Windows
Symantec Endpoint Protection

## 2. INDICE DE PROTECTION

Les résultats suivants reflètent la précision de chaque solution dans la gestion des programmes malveillants uniquement. Ils ne prennent pas en compte les faux positifs.

- **Neutralisation (+1)**

Si la solution a mis fin à une menace, on parle alors de neutralisation. La solution a protégé le système, et a donc gagné un point.

- **Neutralisation, élimination complète (+2)**

La solution a gagné un point de bonus si, en plus d'avoir bloqué le programme malveillant, elle a éliminé toutes les traces de l'attaque.

- **Défense (+3)**

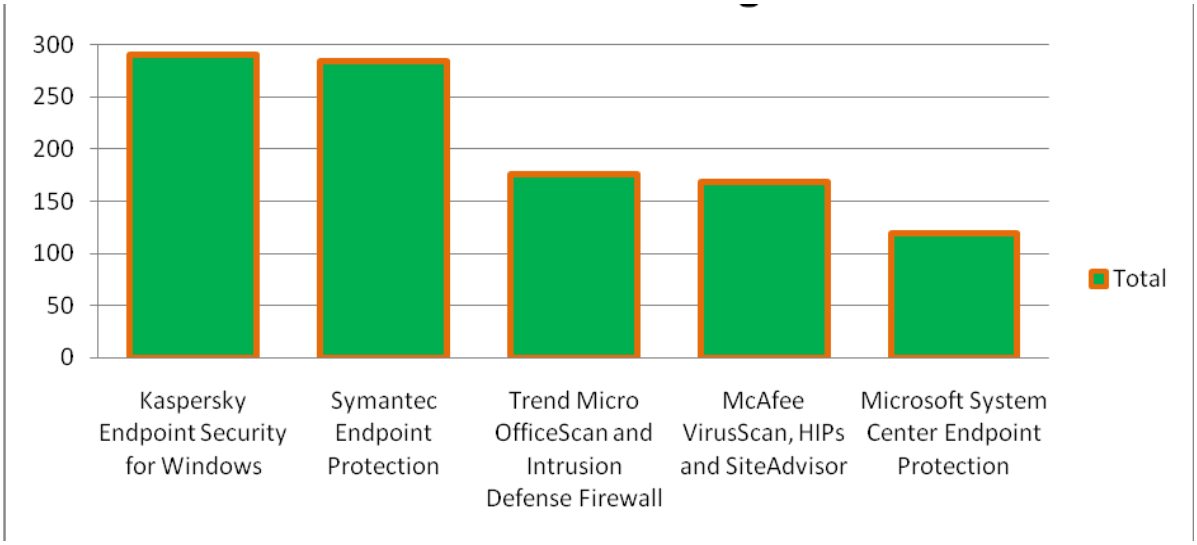
Les solutions qui ont empêché les menaces de se répandre et ainsi « défendu » le système ont gagné trois points.

- **Mise en péril (-5)**

Si la menace s'est répandue dans le système, ou si le système a été endommagé, la solution a perdu cinq points.

Le meilleur indice de protection est de 300, et le plus mauvais est de -500.

**INDICE DE PROTECTION**




**Cet indice de protection reflète les points supplémentaires attribués aux solutions qui ont complètement bloqué la menace, et les points qui ont été perdus lorsqu'une menace a mis le système en péril.**

**Méthode de calcul de l'indice**

Symantec Endpoint Protection s'est défendu 98 fois sur 100. Il n'a neutralisé aucune menace.

Il a gagné trois points à chaque fois qu'il s'est défendu (3x98) et a perdu cinq points à chaque mise en péril (-5x2), son indice final a donc été de 284.

Kaspersky Endpoint Security a obtenu une meilleure note, principalement parce qu'il n'a été mis en péril qu'une seule fois.

Il s'est défendu 98 fois et a neutralisé une menace, sans l'éliminer complètement.

Sa note a été calculée de la façon suivante :

(3x98) + (1x1) + (-5x1) = 290.

La note pondérée récompense les solutions qui empêchent les programmes malveillants de pénétrer dans le système et pénalise lourdement ceux qui ne parviennent pas à empêcher l'infection.

Il est possible d'appliquer votre propre pondération si vous pensez que les mises en péril doivent être plus ou moins pénalisées. Pour ce faire, veuillez utiliser les résultats de *4. Détails de la protection* en page 8.

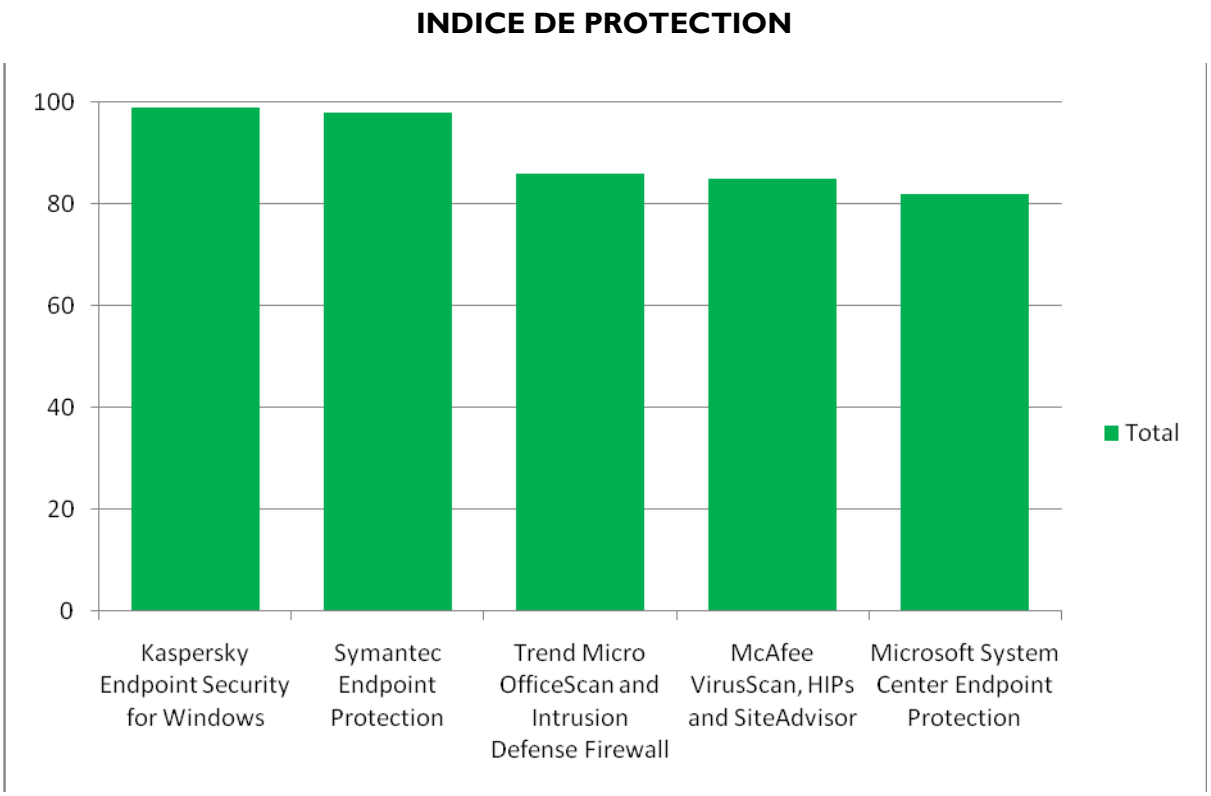
## INDICE DE PROTECTION

| Solution | Indice de protection |
|---|---|
| Kaspersky Endpoint Security for Windows | 290 |
| Symantec Endpoint Protection | 284 |
| Trend Micro OfficeScan et Intrusion Defense Firewall | 176 |
| McAfee VirusScan, HIPs et SiteAdvisor | 168 |
| Microsoft System Center Endpoint Protection | 119 |

## 3. INDICE DE PROTECTION

Les indices suivants reflètent le niveau général de protection, combinant les résultats de défense et de neutralisation.

Aucune distinction n'est faite entre ces différents niveaux de protection. Soit un système est protégé, soit il ne l'est pas.




**L'indice de protection indique simplement combien de fois chaque solution a empêché une menace de pénétrer le système.**

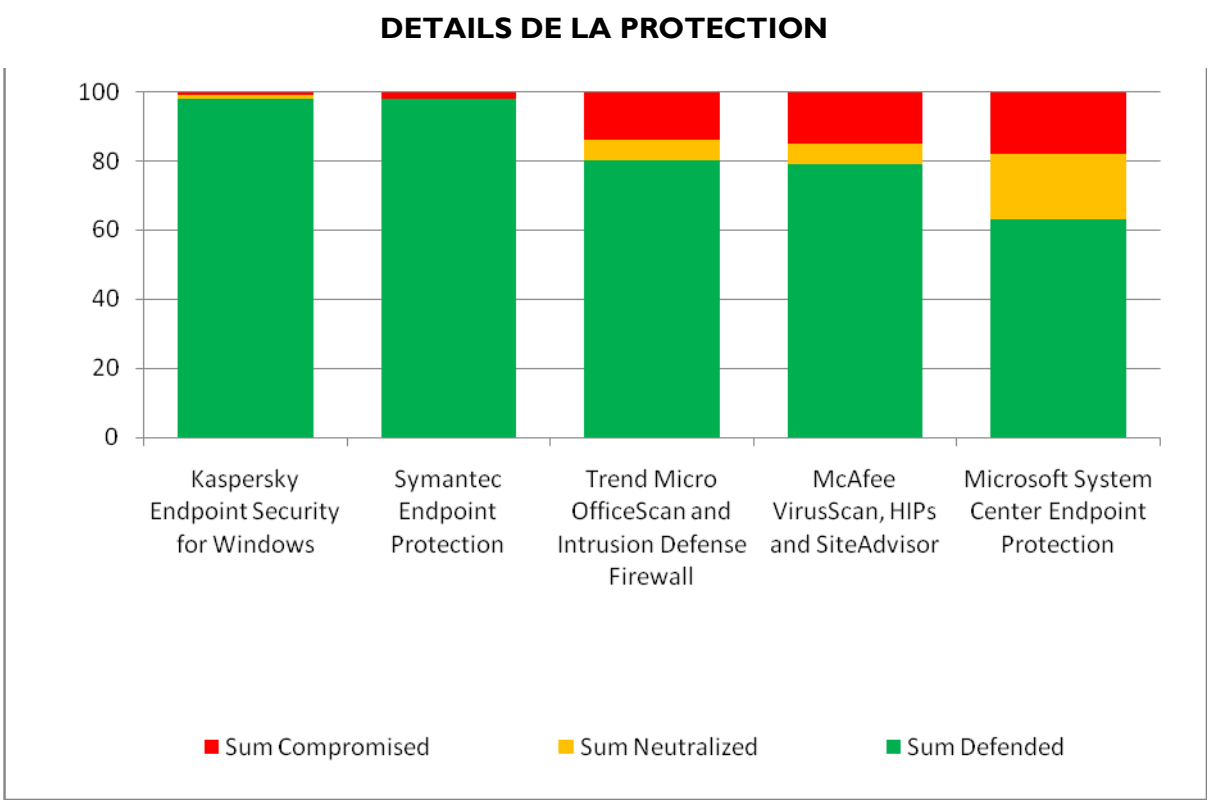
INDICE DE PROTECTION

| Solution | Indice de protection |
|---|---|
| Kaspersky Endpoint Security for Windows | 99 |
| Symantec Endpoint Protection | 98 |
| Trend Micro OfficeScan et Intrusion Defense Firewall | 86 |
| McAfee VirusScan, HIPs et SiteAdvisor | 85 |
| Microsoft System Center Endpoint Protection | 82 |

(Moyenne : 90 %)

## 4. DETAILS DE LA PROTECTION

Les solutions de sécurité ont fourni différents niveaux de protection. Lorsqu'une solution a empêché un programme malveillant d'atteindre le système cible, on dit qu'elle *s'est défendue* contre une menace. Lorsqu'une solution a combattu une menace après que celle-ci ait exploité une vulnérabilité ou infecté le système, on dit qu'elle l'a *neutralisée*. Lorsqu'elle n'y est pas parvenue, le système a été *mis en péril*.




**Le graphique montre la manière dont les solutions ont géré les attaques. Elles sont classées selon leur indice de protection. Pour tous les indices de protection, voir 3. Indice de protection en page 7.**

DÉTAILS DE LA PROTECTION

| Solution | Somme - Défense | Somme - Neutralisation | Somme - Mise en péril |
|---|---|---|---|
| Kaspersky Endpoint Security for Windows | 98 | 1 | 1 |
| Symantec Endpoint Protection | 98 | 0 | 2 |
| Trend Micro OfficeScan et Intrusion Defense Firewall | 80 | 6 | 14 |
| McAfee VirusScan, HIPs et SiteAdvisor | 79 | 6 | 15 |
| Microsoft System Center Endpoint Protection | 63 | 19 | 18 |

# 5. FAUX POSITIFS

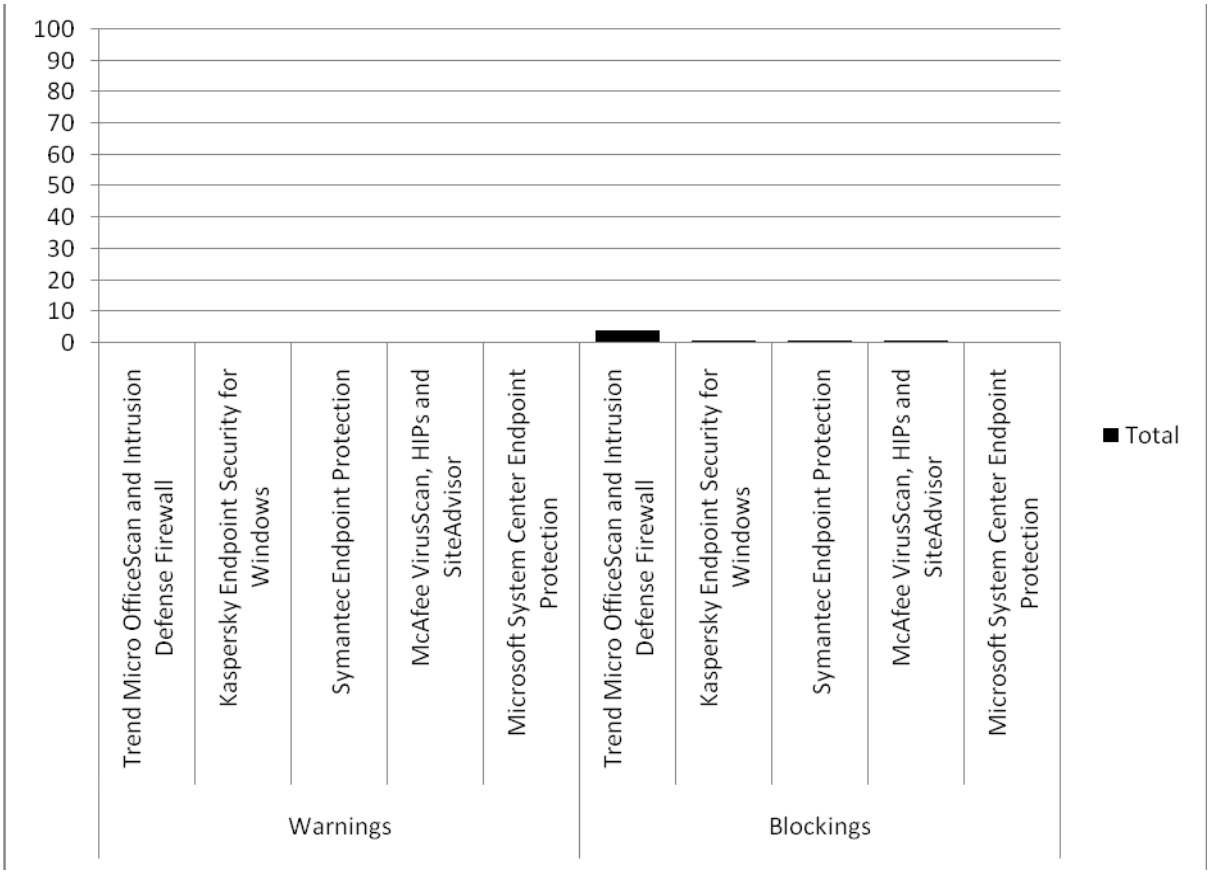
## 5.1 Incidence des faux positifs

Une solution de sécurité doit être capable de protéger le système contre les menaces, tout en permettant aux logiciels authentiques de fonctionner normalement. Lorsqu'un logiciel authentique est classé de façon erronée, un *faux positif* est généré.

Nous avons divisé les résultats en deux grands groupes, car la plupart des solutions que nous avons testées adoptaient l'une des deux approches de base en essayant de protéger un système contre un programme authentique. Soit elles avertissaient que le logiciel était suspect, soit elles décidaient de le bloquer directement.

Le fait de bloquer une application authentique est plus grave que le simple fait d'émettre un avertissement, car cela gêne directement l'utilisateur.

**FAUX POSITIFS**




**Les solutions qui ont généré des faux positifs ont averti les utilisateurs sur le danger d'un logiciel authentique, ou l'ont bloqué complètement.**

INCIDENCE DES FAUX POSITIFS

| Type de faux positifs | Solution | Total |
|---|---|---|
| Avertissements | Trend Micro OfficeScan et Intrusion Defense Firewall | 0 |
| | Kaspersky Endpoint Security for Windows | 0 |
| | Symantec Endpoint Protection | 0 |
| | McAfee VirusScan, HIPs et SiteAdvisor | 0 |
| | Microsoft System Center Endpoint Protection | 0 |
| Blocages | Trend Micro OfficeScan et Intrusion Defense Firewall | 4 |
| | Kaspersky Endpoint Security for Windows | 1 |
| | Symantec Endpoint Protection | 1 |
| | McAfee VirusScan, HIPs et SiteAdvisor | 1 |
| | Microsoft System Center Endpoint Protection | 0 |

## 5.2 Prise en compte de la fréquence des fichiers

La fréquence de chaque fichier est significative. Si une solution classe un fichier commun de façon erronée, cela est plus grave que s'il bloque un fichier moins courant.

Cela étant dit, une solution anti-malwares n'est pas censée bloquer les logiciels authentiques.

Les fichiers sélectionnés pour le test des faux positifs ont été classés en cinq groupes : Très fort impact, Fort impact, Moyen impact, Faible impact et Très faible impact.

Ces catégories sont basées sur le nombre de téléchargements, tel que signalé par les sites de type Download.com au moment du test. Les fourchettes de ces catégories sont indiquées dans le tableau ci-dessous :

FRÉQUENCE DES CATÉGORIES DE FAUX POSITIFS

| Catégorie de l'impact | Fréquence (nombre de téléchargements au cours de la semaine précédente) |
|---|---|
| Très fort impact | >20,000 |
| Fort impact | 1 000 à 20 000 |
| Moyen impact | 100 à 999 |
| Faible impact | 25 à 99 |
| Très faible impact | < 25 |

## 5.3 Modification de l'indice

Les facteurs de modification de l'indice suivants ont été utilisés pour créer un indice de précision pondéré de l'impact. Chaque fois qu'une solution a permis à un nouveau programme authentique de s'installer et de s'exécuter, il a obtenu un point.

À l'inverse, la solution a perdu des points (ou des fractions de points) lorsqu'elle a généré des faux positifs. Nous avons utilisé les facteurs de modification de l'indice suivants :

FACTEURS MODIFIANT L'INDICE DE FRÉQUENCE DES FAUX POSITIFS

| Action en cas de faux positif | Catégorie de l'impact | Facteur de modification de l'indice |
|---|---|---|
| Bloqué | Très fort impact | -5 |
| | Fort impact | -2 |
| | Moyen impact | -1 |
| | Faible impact | -0.5 |
| | Très faible impact | -0.1 |
| Avertissement | Très fort impact | -2.5 |
| | Fort impact | -1 |
| | Moyen impact | -0.5 |
| | Faible impact | -0.25 |
| | Très faible impact | -0.05 |

## 5.4 Répartition dans les catégories d'impacts

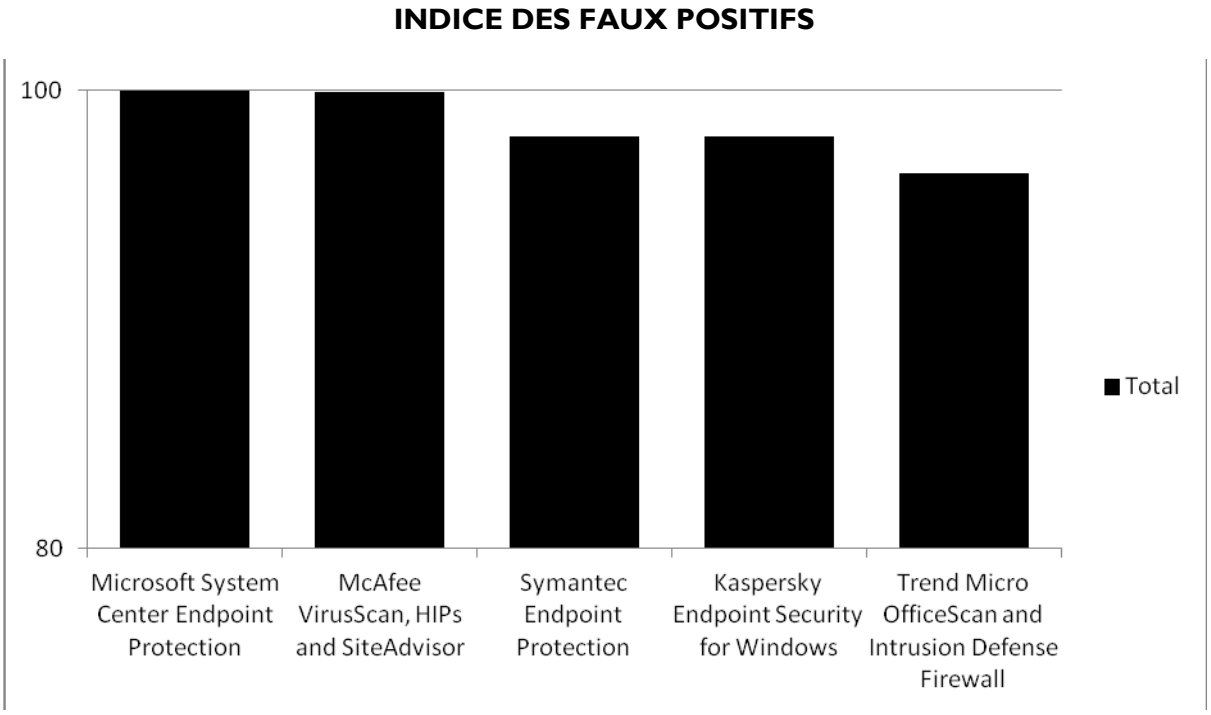
Les solutions ayant obtenu le plus de points sont celles qui ont montré une plus grande précision dans la gestion des applications authentiques utilisées au cours du test. La meilleure note possible était de 100, et la moins bonne de -500 (en partant du principe que toutes les applications ont été classées dans la catégorie Très fort impact, et ont donc été bloquées). Cependant, la répartition des applications dans les catégories d'impacts ne s'est pas limitée à la catégorie Très fort impact. Voici comment les applications ont été réparties :

FRÉQUENCE DES CATÉGORIES DE FAUX POSITIFS

| Taux de fréquence | Fréquence |
|---|---|
| Très fort impact | 27 |
| Fort impact | 38 |
| Moyen impact | 16 |
| Faible impact | 10 |
| Très faible impact | 9 |

## 5.5 Indice des faux positifs

En combinant les catégories d'impacts aux notes pondérées, nous obtenons l'indice de précision des faux positifs suivants.




**Lorsqu'une solution a classé un programme populaire de façon erronée, elle a été plus lourdement pénalisée que si le fichier était moins courant.**

INDICE DES FAUX POSITIFS

| Solution | Indice de précision |
|---|---|
| Microsoft System Center Endpoint Protection | 100 |
| McAfee VirusScan, HIPs et SiteAdvisor | 99.9 |
| Symantec Endpoint Protection | 98 |
| Kaspersky Endpoint Security for Windows | 98 |
| Trend Micro OfficeScan et Intrusion Defense Firewall | 96.4 |

## 6. LES TESTS

### 6.1 Les menaces

Il était important de mettre en place une expérience utilisateur réaliste afin d'illustrer ce qui se passe réellement lorsqu'un utilisateur affronte une cybermenace.

Par exemple, pour ces tests, les logiciels malveillants se trouvaient sur des sites Web infectés originaux, consultés par le biais d'un navigateur Web. Ils n'ont pas été téléchargés depuis un CD ou un site Web interne.

Tous les systèmes cibles ont été entièrement exposés aux menaces. Cela signifie que n'importe quel code de vulnérabilité a pu s'exécuter, ainsi que d'autres fichiers malveillants. Ils se sont exécutés et ont pu fonctionner exactement comme prévu, sous réserve des vérifications réalisées par le logiciel de sécurité installé.

Une durée minimale de cinq minutes a été accordée pour donner au logiciel malveillant l'opportunité d'agir.

### 6.2 Phases de test

Les tests ont été réalisés par phases. Chaque phase a enregistré l'exposition de chaque solution à une menace spécifique. Par exemple, lors de la première phase, chaque solution a été exposée au même site Web malveillant.

À la fin de chaque phase, les systèmes testés ont été complètement restaurés pour éliminer toute trace du logiciel malveillant avant de passer au test suivant.

### 6.3 Surveillance

Une surveillance étroite des systèmes cibles a été nécessaire pour mesurer le succès relatif du logiciel malveillant et de la solution anti-malwares. Cela a inclus l'enregistrement d'activités telles que le trafic réseau, la création de fichiers et processus et les modifications apportées à des fichiers importants.

### 6.4 Niveaux de protection

Les solutions ont affiché différents niveaux de protection. Dans certains cas, la solution a empêché la menace de s'exécuter ou d'apporter une modification significative au système cible.

Dans d'autres cas, la menace a effectué certaines tâches dans le système cible (telle que l'exploitation d'une faille de sécurité ou l'exécution d'un programme malveillant), avant l'intervention et la suppression de tout ou partie du logiciel malveillant par la solution.

Au final, la menace peut contourner la solution de sécurité et effectuer ses activités malveillantes sans entraves. Elle a même pu dans certains cas désactiver la solution de sécurité.

Occasionnellement, le propre système de protection de Windows a géré une menace que la solution antivirus avait ignorée. De même, le logiciel malveillant a pu planter pour plusieurs raisons.

Les différents niveaux de protection fournis par chaque solution ont été enregistrés après analyse des fichiers journaux.

La non-exécution d'un logiciel malveillant pouvant s'expliquer par la présence même d'une solution de sécurité, et non par une mesure de défense spécifique prise par ce dernier, nous lui avons accordé le bénéfice du doute et lui avons attribué la mention Défense.

Si le système testé a été endommagé par une attaque, devenant difficile à utiliser par la suite, il a été considéré comme étant mis en péril, même si les parties actives du logiciel malveillant ont été finalement supprimées par la solution.

### 6.5 Types de protection

Toutes les solutions testées ont fourni deux principaux types de protection : en temps réel et sur demande. La protection en temps réel surveille le système constamment afin de repousser toute menace.

La protection sur demande est essentiellement une « analyse de virus » exécutée par l'utilisateur à un moment donné.

Les résultats du test reflètent le comportement de chaque solution pendant et après l'introduction d'une menace. Le mécanisme de protection en temps réel a été surveillé tout au long du test, tandis que l'analyse sur demande a été exécutée vers la fin de chaque test pour mesurer le niveau de sécurité du système déterminé par la solution.

Les analyses manuelles ont été lancées uniquement lorsqu'un testeur a déterminé qu'un logiciel malveillant avait interagi avec le système cible. En d'autres termes, si la solution de sécurité a réclamé le blocage de l'attaque au stade initial, et que les journaux de surveillance ont fait état de cette demande, le cas a été considéré comme étant clos et la mention Défense a été attribuée.

# 7. DETAILS DU TEST

## 7.1 Les cibles

Afin de créer un environnement de test réaliste, chaque solution a été installée sur un système cible propre Windows XP Professional. Le système d'exploitation a été mis à jour avec Windows XP Service Pack 3 (SP3), sans correctif ou actualisation ultérieurs.

Nous avons effectué les tests sur Windows XP SP3 et Internet Explorer 7 en raison de la forte prédominance des cybermenaces s'exécutant dans cette configuration. Nous voulions également recueillir une année entière de données de tests basés sur Windows XP avant de passer à Windows 7.

La prédominance de ces menaces suggère qu'il existe de nombreux systèmes disposant de ce niveau de correction actuellement connectés à Internet.

Au moment du test, Windows XP était toujours très répandu auprès des utilisateurs (particuliers et entreprises).

Selon Net Applications, qui mesure la popularité des systèmes d'exploitation et des navigateurs Web, les utilisateurs utilisaient Windows XP presque autant que Windows 7. Windows XP était installé sur 39,5 % des PC, tandis que Windows 7 était installé sur 44,4 % des ordinateurs[1].

De plus, notre objectif était de tester la solution de sécurité et non pas la protection fournie par des systèmes entièrement mis à jour avec correctifs et autres mécanismes.

Une sélection de logiciels authentiques, mais vulnérables, a été préinstallée sur les systèmes cibles. Ces derniers présentaient des risques de sécurité connus. Ils incluaient des versions d'Adobe Flash Player, Adobe Reader et Java.

Une solution de sécurité différente a été ensuite installée sur chaque système. Le mécanisme d'actualisation de chaque solution a été utilisé pour télécharger la dernière version de ce dernier.

En raison de la nature dynamique des tests, qui ont été effectués en temps réel avec des sites Web malveillants actuels, les systèmes de mise à jour des solutions ont pu s'exécuter automatiquement et manuellement avant chaque phase de test.

Les solutions programmées pour interroger des bases de données en temps réel ont également été autorisés à le faire. Certaines solutions ont été mise à jour automatiquement au cours du test. La toute dernière version de chaque programme a été utilisée à tout moment du test.

Les systèmes cibles ont utilisé des équipements similaires, dont un processeur Intel Core 2 Duo, 1 RAM de 1 Go, 1 disque dur de 160 Go et un lecteur DVD-ROM. Chaque dispositif a ensuite été connecté à Internet par le biais de son propre réseau virtuel (VLAN) afin d'inviter une infection à croiser des logiciels malveillants.

## 7.2 Sélection des menaces

Les liens vers les sites Web malveillants (URL) utilisés pour les tests n'ont pas été fournis par un éditeur spécifique de solutions anti-malwares.

Ils ont été choisis dans des listes générées par le propre système de détection de sites malveillants de Dennis Technology Labs, qui utilise des mots-clés populaires soumis à Google. Ce système analyse des sites qui apparaissent dans les résultats de recherche depuis un certain nombre de moteurs de recherche et les ajoute à une base de données de sites Web malveillants.

Dans tous les cas, un système de contrôle (Verification Target System - VTS) a été utilisé pour confirmer que les URL étaient bien liées à des sites activement malveillants.

Les URL et fichiers malveillants n'ont été communiqués à aucun des éditeurs au cours du processus de test.

## 7.3 Étapes du test

Chaque test individuel s'est composé de trois étapes principales :

1. Introduction
2. Observation
3. Suppression

Au cours de l'étape *Introduction*, le système cible a été exposé à une menace. Avant l'introduction de la menace, nous avons pris un instantané du système. Cela a généré une liste d'entrées dans le registre et des fichiers sur le disque dur.
La menace a ensuite été introduite.

Immédiatement après l'exposition du système à la menace, le test est passé à l'étape *Observation*.
Au cours de cette étape, qui a duré généralement une dizaine de minutes, le testeur a surveillé le système à la fois visuellement et à l'aide de plusieurs outils tiers.

Le testeur a réagi aux fenêtres contextuelles et autres invités conformément aux directives

[1] http://news.cnet.com/8301-10805_3-57567081-75/windows-8-ekes-out-2.2-percent-market-share/

décrites ci-dessous (voir *7.5 Observation et intervention* ci-dessous).

Cette étape a été abrégée si une activité hostile envers d'autres utilisateurs d'Internet a été observée, telle qu'un spam envoyé par la cible, par exemple.

L'étape *Observation* s'est conclue par un nouvel instantané du système. Cet instantané pris après l'exposition a ensuite été comparé à l'instantané dit « propre » afin de générer un rapport. Le système a été ensuite redémarré.

L'étape *Suppression* a été conçue pour tester la capacité des solutions à nettoyer un système infecté. Si la solution s'est défendue contre la menace au cours de l'étape *Observation*, nous avons omis cette dernière étape. Une analyse sur demande a été exécutée sur la cible, puis un nouvel instantané a été pris. Cet instantané pris après l'analyse a ensuite été comparé à l'instantané dit « propre » afin de générer un rapport.

Tous les fichiers journaliers, dont les rapports générés à partir des instantanés et les propres fichiers journaliers des solutions, ont été récupérés sur la cible.

Dans certains cas cependant, la cible a été tellement endommagée qu'il n'a pas été possible de les récupérer. La cible a ensuite été restaurée dans son état original avant de passer au test suivant.

### 7.4 Introduction des menaces

Les sites Web malveillants ont été visités en temps réel, en passant par un navigateur Web et une connexion Internet lambda. Les URL ont été saisies manuellement dans le navigateur.

Les logiciels malveillants hébergés sur le Web ont tendance à évoluer au fil du temps. Le fait de visiter le même site pendant une courte période peut exposer les systèmes à ce qui peut s'avérer être une série de menaces (bien qu'il puisse s'agir de la même menace, légèrement modifiée pour éviter d'être détectée).

De même, de nombreux sites infectés n'attaqueront une adresse IP particulière qu'une seule fois, ce qui rend difficile le test de plusieurs solutions face à la même menace.

Afin d'améliorer les possibilités que chaque système cible soit exposé au même serveur Web malveillant, nous avons utilisé un système de reproduction Web.

Lorsque les systèmes cibles de vérification ont visité un site malveillant, le contenu de la page incluant le code malveillant a été téléchargé, stocké et chargé sur le système de reproduction. Ainsi, chaque système cible ayant visité le site a été soumis au même contenu.

Les configurations de réseau ont été définies pour offrir un accès libre à Internet à tous les produits pendant toute la durée du test, indépendamment des systèmes de reproduction Web utilisés.

### 7.5 Observation et intervention

Tout au long des tests, le système cible a été observé à la fois manuellement et en temps réel. Cela a permis au testeur de prendre des notes exhaustives sur le comportement perçu du système, et de comparer les alertes visuelles aux entrées consignées dans les fichiers journaliers des solutions.

Pour certaines étapes, nous avons demandé au testeur d'agir comme un utilisateur lambda. Dans un souci de cohérence, le testeur a suivi des directives pour gérer certaines situations, dont le traitement des fenêtres contextuelles affichées par les solutions ou le système d'exploitation, une panne du système, ou des invitations par des logiciels malveillants à réaliser des tâches, etc.

Les directives ont été les suivantes :

1. Agir naïvement. Donner à la menace l'opportunité de s'introduire dans la cible en cliquant sur OK en réponse à des invitations malveillantes, par exemple.
2. Ne pas trop s'entêter à relancer des téléchargements bloqués. Si une solution émet un avertissement sur un site, ne pas essayer d'y accéder par un autre moyen.
3. Si un logiciel malveillant est téléchargé dans un dossier Zip ou autre, l'extraire sur le Bureau, puis l'exécuter. Si le fichier est protégé par un mot de passe que vous connaissez (par ex., mot de passe inclus dans le corps du courriel malveillant original), l'utiliser.
4. Toujours cliquer sur l'option par défaut. Cela s'applique aux fenêtres contextuelles des solutions de sécurité, aux prompts du système d'exploitation (dont le pare-feu de Windows) et aux invitations effectuées par des programmes malveillants.
5. S'il n'y a pas d'option par défaut, attendre. Attendre 20 secondes pour voir si une action est effectuée automatiquement.
6. Si aucune action n'est effectuée automatiquement, choisir la première option. Lorsque les options sont présentées verticalement, choisir la première en partant du haut. Lorsque les options sont présentées horizontalement, choisir la première en partant de la gauche.

## 7.6 Élimination

Lorsqu'une cible est exposée à un logiciel malveillant, la menace peut infecter le système de nombreuses manières. La solution de sécurité peut également protéger la cible de nombreuses manières. Les instantanés expliqués dans la section *7.3 Étapes du test* en page 14 ont fourni des informations qui ont été utilisées pour analyser l'état final d'un système à la fin d'un test.

Un instantané du système cible a été pris avant, pendant et après chaque test pour fournir des informations sur les modifications de ce dernier au cours de son exposition au logiciel malveillant. Par exemple, la comparaison d'un instantané pris avant la visite d'un site Web malveillant avec un instantané pris juste après peut mettre en lumière de nouvelles entrées consignées dans le registre et de nouveaux fichiers sur le disque dur.

Les instantanés ont été également utilisés pour déterminer l'efficacité d'une solution dans l'élimination d'une menace ayant réussi à pénétrer le système cible. Cette analyse souligne les niveaux de protection fournis par une solution.

Ces niveaux de protection ont été classés en trois principaux termes : défendu, neutralisé et mis en péril. Une menace qui n'a pas réussi à atteindre la cible indique que la solution a *défendu* le système; une menace dont les activités ont pu être bloquées a été *neutralisée*, tandis qu'une menace qui a pu atteindre la cible a *mis en péril* le système.

Le système a été défendu si aucune activité malveillante n'est observée à l'œil nu ou par des outils de surveillance tiers à la suite de l'introduction de la menace. Les fichiers de rapport des instantanés sont utilisés pour vérifier cette issue positive.

Si une menace active est observée sur le système, mais ne nécessite par le lancement d'une analyse sur demande, la menace est considérée comme étant neutralisée.

La comparaison des rapports des instantanés doit refléter la création de fichiers malveillants et de nouvelles entrées dans le registre après l'introduction de la menace. Cependant, tant que le rapport d'instantané « analysé » montre que les fichiers ont été supprimés, ou que les entrées de registre ont été éliminées, la menace est considérée comme étant neutralisée.

La cible est mise en péril si l'on constate l'exécution du logiciel malveillant après l'analyse sur demande. Dans certains cas, une solution peut requérir l'exécution d'une analyse supplémentaire afin de procéder à l'élimination. Ces analyses secondaires sont acceptables, mais les demandes d'analyse continues peuvent être ignorées si aucune progression n'est observée.

Le système a été mis en péril si un fichier « hôte » a été modifié ou si un fichier du système a été altéré.

## 7.7 Surveillance automatique

Les fichiers journaliers ont été générés par des applications tierces, ainsi que par les solutions de sécurité.

L'observation manuelle du système cible tout au long de son exposition au logiciel malveillant (et autres applications authentiques) a fourni plus d'information sur le comportement des solutions de sécurité.

La surveillance a été effectuée directement sur le système cible et sur le réseau.

### Journalisation côté client

Une combinaison de Process Explorer, Process Monitor, TcpView et Wireshark a été utilisée pour surveiller les systèmes cibles. Regshot a été utilisé entre chaque étape du test afin de capturer un instantané du système.

Un certain nombre de scripts créés par Dennis Technology Labs ont également été utilisés pour fournir des informations supplémentaires sur le système. Chaque solution a généré un certain niveau de journalisation.

Process Explorer et TcpView ont été exécutés tout au long des tests, fournissant une aide visuelle au testeur sur les activités potentiellement malveillantes observées sur le système. En outre, les informations consignées en temps réel par Wireshark, et l'affichage sur le web proxy (voir journalisation de l'activité réseau, ci-dessous), ont révélé des activités réseau spécifiques, telles que des téléchargements secondaires.

Process Monitor a également fourni de précieuses informations pour aider à reconstituer les incidents malveillants. Process Monitor et Wireshark ont tous deux été configurés pour sauvegarder automatiquement leurs journaux dans un fichier. Cela a permis de réduire la perte des données lorsqu'un logiciel malveillant a provoqué l'interruption ou le redémarrage du système.

### Journalisation de l'activité réseau

Tous les systèmes cibles ont disposé d'une connexion à Internet, munie d'un proxy web et d'un système de surveillance réseau. Tout le trafic vers et depuis Internet devait passer par ce système.

Le système de surveillance réseau était un système Linux à double résidence, fonctionnant comme un routeur transparent, acheminant tout le trafic Web à travers un proxy Squid.

Un système de reproduction HTTP s'est assuré que tous les systèmes cibles seraient soumis au même logiciel malveillant. Il a été configuré pour permettre l'accès à Internet pour que les solutions puissent télécharger les mises à jour et communiquer avec tous les serveurs disponibles « dans le cloud ».

# 8. CONCLUSIONS

- **Où se trouvent les menaces ?**

Les menaces utilisées au cours de ce test étaient authentiques et réelles, et infectaient les ordinateurs des victimes à l'international au moment même où nous testions les solutions. Dans la plupart des cas, la menace a été lancée à partir d'un site Web authentique infecté.

Les types de sites malveillants ou infectés étaient variés, ce qui démontre qu'un logiciel anti-malwares efficace est essentiel pour tous ceux qui veulent naviguer sur le Web depuis un PC équipé de Windows.

La plupart des menaces se sont installées automatiquement au moment où un utilisateur a visité une page Web infectée. Cette infection était souvent invisible à l'œil d'un observateur non averti.

- **Où commence la protection ?**

Il y a eu un nombre significatif de mises en péril au cours de ce test, ainsi qu'un nombre relativement élevé de neutralisations.

Les solutions les plus robustes ont bloqué le site avant même qu'il ne puisse attaquer. Les solutions les plus faibles ont eu tendance à gérer la menace une fois que celle-ci a commencé à interagir avec le système cible.

- **Séparer le bon grain de l'ivraie**

Kaspersky Endpoint Security for Windows a obtenu la meilleure note en termes de protection contre les programmes malveillants, suivi de près par Symantec Endpoint Protection.

La solution Kaspersky a été mise en péril une seule fois, Symantec par deux fois, et les autres produits entre 14 et 18 fois.

Microsoft System Center Endpoint Protection a démontré une performance particulièrement faible dans la détection de programmes malveillants et n'a protégé le système que dans 82 % des cas.

Les solutions anti-malwares doivent être capables de faire la différence entre un programme malveillant et un qui ne l'est pas. La solution de Trend Micro a été légèrement inférieure par rapport aux solutions concurrentes, générant quatre faux positifs. Ce qui reste un nombre faible.

Microsoft System Center Endpoint Protection a été la seule solution n'ayant pas généré de faux positifs.

Globalement, en prenant en compte la capacité de chaque solution à gérer à la fois les applications malveillantes et authentiques, les gagnants sont sans appel Kaspersky Endpoint Security for Windows et Symantec Endpoint Protection.

- **L'antivirus est important (mais n'est pas la panacée)**

Ce test démontre que même sur un échantillon relativement petit de 100 menaces, il existe une différence de performance significative entre les différents programmes antivirus. De même, il illustre cette différence en se basant sur des menaces réelles qui ont attaqué des ordinateurs réels au moment du test.

Le niveau de protection moyen des solutions testées a été de 90 % (voir *3. Indice de* protection en page 7).

Ce pourcentage est bien inférieur aux résultats généralement indiqués sur certaines documentations marketing de ces solutions anti-malwares.

La simple présence d'une solution anti-malwares peut être perçue comme suffisante pour diminuer les chances d'infection par un logiciel malveillant, même lorsque les seuls sites visités sont connus comme étant activement malveillants. Cela étant dit, aucune solution n'a atteint un taux de protection de 100 %.

## ANNEXE A : TERMES EMPLOYES

| | |
|---|---|
| Cible | Système testé exposé à des menaces, afin de surveiller le comportement des solutions de sécurité. |
| Défendu | Le logiciel malveillant n'a pas réussi à s'exécuter ou à modifier la cible. |
| Suppression | Étape du test qui mesure les capacités d'une solution à éliminer toute menace installée. |
| Protection en temps réel | La protection toujours active offerte par de nombreuses solutions de sécurité. |
| Faux positif | Une application authentique est classée de manière erronée comme étant malveillante. |
| Instantané | Enregistrement d'un système de fichier cible et de contenu dans un registre. |
| Introduction | Étape du test où un système cible est exposé à une menace. |
| Prompt (message) | Questions posées par un logiciel, dont le logiciel malveillant, les solutions de sécurité et le système d'exploitation. Les prompts des solutions de sécurité apparaissent généralement sous la forme d'une fenêtre contextuelle. Certains prompts ne posent pas de questions, mais affichent un message d'alerte. Lorsque ces messages apparaissent et disparaissent sans requérir d'action de la part de l'utilisateur, on les appelle des « toasters ». |
| Menace | Un programme conçu pour endommager un système. |
| Mis en péril | Le logiciel malveillant continue à s'exécuter sur un système infecté, même après l'exécution d'une analyse sur demande. |
| Mise à jour | Code fourni par un éditeur pour maintenir ses logiciels à jour. Cela inclut les définitions de virus, des mises à jour et des correctifs du système d'exploitation. |
| Neutralisé | Le logiciel malveillant ou code exploitant une vulnérabilité a atteint la cible, mais a été ensuite supprimé par la solution de sécurité. |
| Observation | Étape du test au cours de laquelle le logiciel malveillant est susceptible d'affecter la cible. |
| Phase | Série de tests menés sur différentes solutions , visant à exposer chaque cible à la même menace. |
| Protection sur demande | Analyse manuelle du virus, exécutée par l'utilisateur à un moment donné. |

## ANNEXE B : FAQ

- Ce test n'a pas été sponsorisé.
- Les phases de test ont été réalisées entre le 10 Avril et le 12 Juin 2013 à l'aide de la version la plus récente du logiciel disponible à un moment donné.
- Toutes les solutions ont été en mesure de communiquer avec leurs systèmes de soutien sur Internet.
- Les solutions sélectionnées pour ce test ont été choisies par Dennis Technology Labs.
- Les échantillons ont été rassemblés et vérifiés par Dennis Technology Labs.
- Les solutions ont été exposées aux menaces dans un délai de 24 h après que ces dernières aient été vérifiées. En pratique, le délai n'a été généralement que de trois ou quatre heures.
- Les détails des échantillons, dont leur URL et leurs codes, ont été fournis aux partenaires seulement à la fin du test.
- Les échantillons étaient composés de 100 URL activement malveillantes et de 100 applications authentiques.

**Les éditeurs participants ont-ils été informés des échantillons destinés au test, avant ou pendant ce dernier ?**
Non. Nous ne savions pas nous-mêmes quelles menaces seraient utilisées avant le début du test. Nous en découvrions de nouvelles chaque jour, il nous était donc impossible de fournir ce type d'informations avant le début du test. Nous n'avons divulgué ces informations qu'à la fin du test.

**Quelle est la différence entre un éditeur et un éditeur partenaire ?**
Les éditeurs partenaires ont contribué financièrement au test en échange d'une prévisualisation des résultats, d'une opportunité de contester les résultats avant leur publication et du droit d'utiliser le logo de la récompense sur leur outil marketing. Les autres participants ont découvert les résultats le jour de leur publication et n'ont pas été autorisés à utiliser le logo de la récompense.

**Avez-vous fourni les échantillons aux éditeurs ?**
Les éditeurs partenaires ont pu télécharger tous les échantillons à la fin du test.

Les éditeurs ont pu solliciter un échantillon des menaces ayant mis en péril leurs solutions s'ils souhaitaient vérifier nos résultats par eux-mêmes. Il en va de même pour les journaux côté client, dont les fichiers de capture réseau. (Service soumis à des frais supplémentaires minimes).

**Qu'est-ce qu'un échantillon ?**
Dans nos tests, un échantillon n'est pas seulement un ensemble de fichiers exécutables malveillants qui s'exécutent sur le système. Un échantillon est une archive complète de reproduction qui permet aux testeurs de répliquer l'incident, même si le site Web infecté original n'est plus disponible. Cela signifie qu'il est possible de reproduire l'attaque et de déterminer quelle a été la couche de protection défaillante. La reproduction de l'attaque doit, dans la plupart des cas, aboutir aux fichiers exécutables pertinents. Dans le cas contraire, ces fichiers sont généralement disponibles sur le fichier de capture réseau côté client (pcap).