Symantec™ Endpoint Protection 12.1.5
Fiche technique

Fiche technique : Sécurité des terminaux

Présentation

Outre les attaques massives à grande échelle qu'ils perpétuent, les logiciels malveillants ont évolué et incluent désormais des attaques ciblées et des menaces persistantes avancées qu'un simple antivirus ne peut arrêter. N'attendez plus pour aller au-delà d'une simple protection antivirus. Symantec est le seul à pouvoir proposer des fonctionnalités de sécurité intelligente qui tirent parti de la communauté d'utilisateurs du Global Intelligence Network (GIN), le plus important réseau de données au monde qui collecte des données issues des systèmes de millions d'utilisateurs et de capteurs. Bénéficiant des données de ce réseau, la technologie exceptionnelle Insight™ de Symantec™ Endpoint Protection bloque les menaces en mutation et accélère le temps d'analyse en identifiant la réputation des fichiers. En parallèle, la technologie SONAR™ bloque les menaces de type « zero-day » en surveillant les comportements des fichiers en temps réel. Grâce à un agent hautes performances qui intègre des technologies de sécurité intelligentes, un logiciel antivirus puissant et une fonctionnalité de verrouillage des politiques, Symantec™ Endpoint Protection 12.1.5 permet de vous concentrer sur votre activité sans compromettre la sécurité ou les performances.

Sécurité inégalée

Protection contre les attaques ciblées et les menaces persistantes avancées en s'appuyant sur une sécurité intelligente et une protection multi-couches qui va au-delà d'un simple antivirus.

- Tire parti du Global Intelligence Network (GIN), le plus important réseau de données au monde composé de centaines de millions de capteurs alimentant nos technologies de protection proactives en données.
- Bénéficiant des données de ce réseau, la technologie Insight™ unique identifie la réputation des fichiers en analysant les attributs des fichiers clés, notamment la fréquence de téléchargement d'un fichier, le temps de présence d'un fichier et la source de téléchargement. Grâce à ces informations, nous sommes en mesure de bloquer davantage de menaces et d'assurer la protection contre des logiciels malveillants nouveaux et mutants.
- La technologie SONAR™, reposant également sur le réseau GIN, surveille le comportement des applications en temps réel et bloque les attaques ciblées et les menaces de type « zero-day ».
- La solution de protection contre les menaces réseau analyse les données entrantes qui arrivent sur l'ordinateur d'un utilisateur via des connexions réseau et bloque les menaces avant qu'elles n'atteignent le système.
- Symantec™ Endpoint Protection détecte et supprime davantage de menaces qu'aucune autre solution de sa catégorie[1], obtenant à plusieurs reprises la note la plus élevée dans le classement AAA selon le test antivirus dans le « monde réel » réalisé par Dennis Technology Labs.

Performances optimales

Des performances si exceptionnelles que les utilisateurs ne remarquent pas sa présence.

- La technologie Insight™ de Symantec intégrée à Endpoint Protection élimine jusqu'à 70 % de la charge d'analyse demandée par les solutions traditionnelles en identifiant précisément la réputation des fichiers. Ainsi seuls les fichiers à risques sont analysés.
- Fonctionnement plus rapide et durée de vie plus longue du matériel grâce à un impact système réduit.
- Réduction de la charge réseau grâce à un contrôle flexible sur le nombre de connexions et la bande passante.
- Surpasse tous les produits de sa catégorie en termes de vitesse d'analyse et de performances globales[2].

1 TEST ANTIVIRUS, avis sur les produits, solutions d'entreprise pour Windows 7, juillet/août 2013.
2 PassMark Software, « Tests de performance des solutions de sécurité des terminaux pour les entreprises », 2014.

Symantec

Gestion plus intelligente

Console de gestion unique sur les plates-formes physiques et virtuelles avec contrôle granulaire des politiques.

- Technologies de sécurité intelligentes et fonctionnalités de verrouillage des politiques intégrées à un agent hautes performances unique contrôlé par une seule console de gestion sur PC, Mac, Linux et machines virtuelles.
- Contrôle granulaire des politiques et possibilité de personnaliser des politiques en fonction des utilisateurs et de leur emplacement.
- Prise en charge des déploiements à distance et de la gestion client pour PC et Mac, facilitant ainsi la mise à jour des terminaux distants.
- Reporting avancé grâce à l'intégration d'analyses multidimensionnelles et de rapports graphiques présentés dans un tableau de bord simple à utiliser.
- Le fournisseur de mises à jour groupées réduit la charge réseau ainsi que le temps nécessaire à l'obtention des mises à jour en permettant à un client d'envoyer des mises à jour à un autre. Ainsi, les mises à jour sont plus efficaces sur les sites distants.

---

5 niveaux de protection

Symantec™ Endpoint Protection 12.1.5 offre **5 niveaux de protection** : 1) réseau 2) fichiers 3) réputation 4) comportement et 5) réparation :

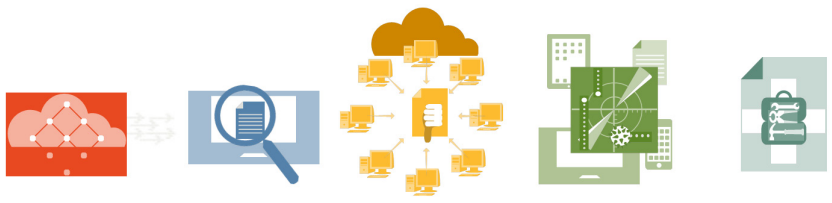
1) Réseau : la protection contre les menaces réseau de Symantec intègre la technologie *Vantage* qui analyse les données entrantes et bloque les menaces circulant sur le réseau avant qu'elles n'atteignent le système. Un pare-feu basé sur des règles ainsi qu'une protection du navigateur sont également inclus pour vous protéger des attaques Web.

2) Fichiers : un antivirus basé sur des signatures recherche et élimine les programmes malveillants d'un système afin de le protéger contre les virus, les vers informatiques, les chevaux de Troie, les logiciels espions, les bots, les logiciels publicitaires et les rootkits.

3) Réputation : la technologie *Insight™* met en corrélation des dizaines de milliards de liens entre les utilisateurs, les fichiers et les sites Web afin de détecter les menaces qui mutent rapidement. En analysant les attributs des fichiers clés, Insight™ est en mesure d'identifier si un fichier est sûr et lui attribue un score de réputation. Vous bénéficiez ainsi d'une protection efficace contre les attaques tout en réduisant la charge d'analyse de 70 %.

4) Comportement : la technologie SONAR™ exploite l'intelligence artificielle afin d'assurer une protection contre les attaques « zero-day ». Elle bloque les menaces inconnues en surveillant près de 1 400 comportements de fichiers pendant leur exécution en temps réel afin de déterminer le risque lié aux fichiers.

5) Réparation : Power Eraser™ analyse de manière active les terminaux infectés afin de localiser les menaces persistantes avancées et de supprimer les logiciels malveillants tenaces. La prise en charge à distance permet aux administrateurs de déclencher l'analyse Power Eraser et de traiter l'infection à distance depuis la console de gestion de Symantec™ Endpoint Protection.



Pare-feu et prévention contre des intrusions
Réseau
Bloque les logiciels malveillants avant qu'ils ne se propagent sur votre machine et contrôlent le trafic

Antivirus
Fichier
Analyse et supprime les programmes malveillants qui arrivent sur un système

Insight
Réputation
Détermine la sécurité des fichiers et des sites Web en s'appuyant sur la communauté d' utilisateurs

Sonar
Comportements
Surveille et bloque les programmes qui présentent des comportements suspects

Power eraser
Réparation
Traitement actif des infections tenaces

Fonctionnalités de contrôle des politiques étendues

Outre les technologies de protection de base, Symantec™ Endpoint Protection 12.1.5 offre également la possibilité d'effectuer des contrôles des politiques granulaires, notamment :

1) Verrouillage des systèmes : renforce la protection des systèmes stratégiques en autorisant uniquement l'exécution d'applications sûres figurant sur une liste blanche ou en bloquant l'exécution des applications à risques répertoriées sur une liste noire.

2) Contrôle des applications et des périphériques : permet d'empêcher les atteintes à la sécurité internes et externes en surveillant le comportement des applications et en contrôlant l'accès aux fichiers, aux registres, les processus pouvant s'exécuter et les informations relatives aux périphériques pouvant y être inscrites.

3) Vérification de l'intégrité de l'hôte et application des politiques : permet aux utilisateurs d'exécuter des scripts sur leurs terminaux afin de vérifier et de rendre compte de la conformité ; zone de quarantaine, verrouillage de partage de fichiers et isolement d'un système non conforme ou infecté.

4) Identification du lieu de connexion : détecte automatiquement le lieu depuis lequel un système se connecte, tel qu'un hôtel, un point d'accès, un réseau sans fil ou un réseau privé virtuel (VPN) et règle les paramètres de sécurité afin d'offrir la protection la plus efficace adaptée à l'environnement.

Verrouillage des systèmes
Contrôle strict des applications par le biais de listes blanches et de listes noires

Contrôle des applications
Surveille et contrôle le comportement des applications

Contrôle des périphériques
Limite et autorise l'accès au matériel pouvant être utilisé

Intégrité de l'hôte
Garantit la protection et la conformité des terminaux

Optimisation virtuelle

Symantec™ Endpoint Protection protège vos environnements virtuels haute densité tout en maintenant des niveaux de performance supérieurs aux solutions sans agent et en offrant une visibilité globale de la sécurité.

1) Intégration de VMware vShield : densité de machines virtuelles plus élevée et réduction de l'utilisation des E/S et du processeur.

2) Exception d'image virtuelle : placement des fichiers sur une liste blanche depuis l'image d'une machine virtuelle standard en vue d'optimiser l'analyse.

3) Optimisation des ressources : exécution aléatoire d'analyses et de mises à jour planifiées afin d'éviter les pics d'utilisation des ressources.

4) Cache Insight™ partagé : analyse unique des fichiers, partage des résultats entre les clients et déduplication de l'analyse des fichiers afin de réduire la bande passante et le temps de latence.

5) Identification des clients virtuels : détection et gestion automatiques des environnements virtuels pour définir plus facilement des politiques spécifiques pour les machines virtuelles.

6) Analyse d'images hors connexion : détecte les menaces à partir d'images de machines virtuelles hors connexion.

7) Limitation des analyses pour la virtualisation : détecte la charge disque et réduit la vitesse d'analyse afin d'éviter les pics d'utilisation.

Configuration requise pour postes de travail clients et serveurs
Systèmes d'exploitation Windows
Windows XP (32 bits, SP2 ou version ultérieure, 64 bits)
Windows XP Embedded (SP2 ou version ultérieure)
Windows Vista (32 bits, 64 bits)
Windows 7 (32 bits, 64 bits)
Windows 7 Embedded
Windows 8 (32 bits, 64 bits)
Windows Server 2003 (32 bits, 64 bits, R2 ou SP1 ou version ultérieure)
Windows Server 2008 (32 bits, 64 bits, y compris R2)
Windows Server 2012 (32 bits, y compris R2)
Windows Small Business Server 2011 (64 bits)
Windows Essential Business Server 2008 (64 bits)
Systèmes d'exploitation Macintosh
MAC OS X 10.6.8, 10.7, 10.8, 10.9
MAC OS X Server 10.6, 10.7, 10.8, 10.9
Systèmes d'exploitation Linux (versions 32 bits et 64 bits)
Red Hat Enterprise Linux
SUSE Linux Enterprise (server/desktop)
Novell Open Enterprise Server
Oracle Linux
VMWare ESX
Ubuntu
Debian
Fedora
Environnements virtuels
vSphere Server (ESXi)
Microsoft Hyper-V
Citrix XenServer, XenDesktop, XenApp
Configuration matérielle
Processeur 1 GHz ou supérieur
512 Mo de RAM (1 Go recommandé)
850 Mo d'espace disponible sur le disque dur

Configuration requise pour Endpoint Protection Manager
Systèmes d'exploitation Windows
Windows 7
Windows XP (32 bits, SP3 ou version ultérieure, ou 64 bits, SP2 ou version ultérieure)
Windows Server 2003 (32 bits, 64 bits, R2 ou SP1 ou version ultérieure)
Windows Server 2008 (32 bits, 64 bits, y compris R2)
Windows Small Business Server 2008 (64 bits)
Windows Small Business Server 2011 (64 bits)
Windows Essential Business Server 2008 (64 bits)
Windows Server 2012 (64 bits, y compris R2)
Matériel
Processeur 1 GHz ou supérieur
1 Go de RAM (2 Go recommandé)
16 Go ou plus d'espace disponible sur le disque dur
Navigateur Internet
Microsoft Internet Explorer
Mozilla Firefox
Base de données
Base de données intégrée incluse ou sélectionnez la vôtre dans la liste suivante : SQL Server 2005, SP4 ou version ultérieure SQL Server 2008 et R2 SQL Server 2012 SQL Server 2014

* Pour obtenir une liste complète des configurations requises, veuillez consulter la page d'assistance

Essai gratuit

Essayez la solution leader en matière de protection des terminaux en téléchargeant une version d'essai gratuite de 30 jours dès aujourd'hui :

http://www.symantec.com/endpoint-protection/trialware

Consultez les avis tiers et découvrez les raisons pour lesquelles Gartner a classé Symantec en tant que leader dans le Magic Quadrant pour les plates-formes de protection des terminaux :

http://www.symantec.com/endpoint-protection/news-reviews

Informations complémentaires

Visitez notre site Web

http://enterprise.symantec.com

Pour entrer en contact avec l'un de nos spécialistes produit hors des États-Unis

Appel gratuit : 1 (800) 7456054

Pour entrer en contact avec l'un de nos spécialistes produit hors des États-Unis

Pour obtenir les adresses et numéros de téléphone de nos agences locales, visitez notre site Web.

À propos de Symantec

Symantec protège les informations échangées à travers le monde et se positionne comme leader mondial des solutions de sécurité, de sauvegarde et de disponibilité. Nos produits et services innovants protègent les individus et les informations dans n'importe quel environnement, du plus petit appareil mobile aux data centers et systèmes dans le cloud. Notre expertise mondialement reconnue en matière de protection des données, des identités et des échanges permet à nos clients de travailler en toute confiance dans le monde connecté d'aujourd'hui. Pour plus d'informations, rendez-vous sur www.symantec.com ou rejoignez Symantec sur : go.symantec.com/socialmedia.

Siège mondial de Symantec

350 Ellis St.
Mountain View, CA 94043 États-Unis
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

21320633-2FR 07/14