

INTÉGRATION DE LA SÉCURITÉ

Défi pour les entreprises

La nature variable des menaces nécessite une approche mult niveau de la protection antivirus afin d'empêcher les malwares d'infecter les ordinateurs ou de se propager sur les réseaux d'entreprise par courriel ou via Internet. Le marché foisonne d'appiances et d'applications autonomes, cependant le défi consiste à intégrer une défense solide contre les malwares sans que cela ait un impact retentissant sur les performances ou sur les frais de développement.

La solution Sophos

Intégration transparente

SAV Interface™ permet aux utilisateurs d'un large éventail d'applications autonomes de bénéficier d'une intégration accélérée avec le moteur de détection virale de Sophos. Cette intégration à la passerelle de technologies de pointe signifie que l'entreprise protège en toute transparence son réseau contre les virus, chevaux de Troie, vers, spywares et adwares.

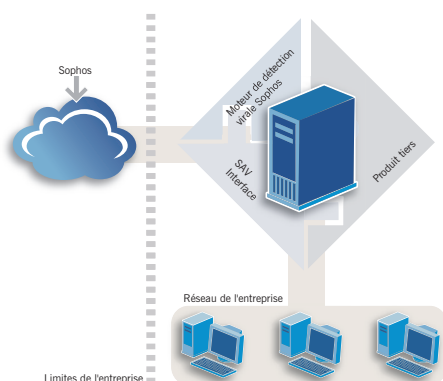
Protection plébiscitée contre les malwares

L'intégralité du trafic transitant par l'application tierce, qu'il s'agisse du trafic Internet ou de courriels, pièces jointes compressées comprises, est vérifié pour y déceler la présence éventuelle de malwares. La technologie Genotype® de détection des virus bloque proactivement

les familles de virus tandis que Behavioral Genotype Protection assure une protection automatique contre les menaces du jour en analysant leur comportement avant que leur code ne s'exécute. Les fichiers d'identités des malwares écrits par les SophosLabs™ sont entièrement mis à jour via Internet.

Administration simplifiée

Cette robuste protection s'accompagne d'avantages considérables en matières de performances car SAV Interface n'a besoin que d'une copie de la base de données sur les informations virales pour satisfaire à toutes les demandes. Ce qui signifie que les fréquentes opérations de chargement et de réinitialisation exigées par les scanners par lignes de commande ne sont plus nécessaires.



SAV Interface : protection antivirus intégrée à la passerelle

Avantages principaux

- » Possibilité pour l'utilisateur d'applications tierces d'une intégration accélérée avec le moteur de détection virale Sophos.
- » Possibilité pour les applications passerelles de surveiller en temps réel le trafic de courriels ainsi que les trafics Internet et FTP.
- » Détection des menaces connues et inconnues, y compris virus, chevaux de Troie, vers et spywares.
- » Détection des malwares dans les pièces jointes compressées des courriels, archives récursives comprises.
- » Protection de la passerelle sans impact sur la productivité de l'utilisateur final.
- » Amélioration considérable des performances par rapport aux scanners de virus par lignes de commande traditionnels.
- » Intégration simplifiée grâce aux nombreuses méthodes et différentes langues.
- » Alerte de l'administrateur en cas de détection virale.
- » Mise à jour automatique (environ 5 Ko) avec la plus récente protection délivrée par les SophosLabs™, réseau international de centres d'analyse des menaces.
- » Élimination de l'excès d'utilisation mémoire par l'utilisation d'une seule copie multiprocesseur du moteur de détection virale pour traiter toutes les demandes.
- » Support technique 24/7 pendant toute la durée de validité de la licence et possibilité de contacter Sophos à tout moment pour une assistance individuelle.

INTÉGRATION DE LA SÉCURITÉ

Détails techniques

Fonction

- Interface vers le moteur de détection virale de Sophos.

Technologies antivirus

- Une variété de technologies, incluant Dynamic Code Analysis™, la recherche de motifs, l'analyse par émulation et l'analyse heuristique recherchent automatiquement le code malveillant.
- Blocage proactif de familles de virus via la technologie de détection par génotype.
- La technologie Behavioral Genotype Protection assure automatiquement votre défense contre les menaces du jour zéro en analysant leur comportement avant que leur code ne s'exécute. Les séries de règles comportementales Sophos sont constamment examinées avec pour référence une bibliothèque d'applications légitimes permettant de réduire les risques de faux positifs.

Mise à jour de la protection antivirus

- La mise à jour de la protection antivirus s'effectue automatiquement.

Interface

- Possibilité d'utiliser un lien direct (SAV Interface SDK) ou un processus daemon (SAV Dynamic Interface).
- SAV Interface SDK utilise une interface C/C++ de type COM sur toutes les versions pour une cohérence inter-plates-formes. Les applications tierces utilisent des fonctions de rappel dans la bibliothèque de SAV Interface pour fonctionner avec le moteur de détection virale.
- SAV Dynamic Interface est une interface générale qui s'intègre en plusieurs langues.

Mode de fonctionnement

- Windows®, OS/2 : Dynamic Link Library (DLL) compatible COM ou service non conforme sans processus.
- Mac OS X : Framework.
- Plates-formes UNIX, OpenVMS : bibliothèque partagée se présentant sous forme binaire ou en réseau API.
- NetWare : NetWare Loadable Modules (NLM).

Mémoire nécessaire

- SAV Interface : 25–30 Mo de RAM (données virales incluses).

Espace disque

- SAV Interface : 10–12 Mo (données virales incluses).

Vitesse de contrôle

- 20–30 fois meilleure qu'avec un scanneur par lignes de commande.
- Temps de contrôle type d'un fichier en mode normal < 20 millisecondes.

Pour évaluer SAV Interface, visitez www.sophos.fr/products

Remarque : une liste complète d'intégrateurs est disponible sur www.sophos.fr/partners/oem. Le kit de développement de logiciels SAV Interface, SAV Dynamic Interface ainsi que des informations techniques sont aussi disponibles.

Configuration nécessaire

» Windows

Windows 2000/XP/2003/Vista
Windows 95/98/Me et NT4

» Mac OS X

OS X 10.2/10.3/10.4

» Linux sur Intel

Red Hat 5.1/5.2/6.0/6.1/7.2/8.0/
9.0, RHEL 2.03/01/04
SUSE 07/06/08/9.0/9.1/9.2/
9.3/10.0, Enterprise Server 8/9
TurboLinux 07/06/08/10

» FreeBSD

3.0/3.4/4.0/4.5/4.8/5.1/5.2/5.3
/5.06/04/06.1 sur Intel, 6.0 sur
AMD64

» OpenBSD

3.6/3.7/3.8 sur Intel et sur
AMD64

» HP-UX

10.20/11.0/11.11/11.23 sur
HP-PA, 11.23 sur Itanium 2

» AIX

4.2/5.1/5.2/5.3 sur PowerPC

» Solaris

Solaris 08/07/09/10 sur Intel
Solaris 09/08/10 sur SPARC
Sun OS 5.6 sur SPARC

» SCO

UnixWare 7.0 à 7.1.4 sur Intel
OpenServer 5.0.5/5.0.7/6 sur
Intel

» OS/2

Warp version 3/4

» OpenVMS

5.4-3 sur VAX
1.5 à 7.x sur Alpha
8.2 sur Itanium 2

» NetWare

4.2/5.0/5.1/6.0/6.5,
Open Enterprise Server

Sophos est l'un des plus grands éditeurs mondiaux de solutions de sécurité et de contrôle informatiques. Nous offrons la protection et le contrôle aux entreprises et aux organisations éducatives et gouvernementales – en assurant leur défense contre les malwares connus et inconnus, les spywares, les intrusions, les applications indésirables, le spam et les violations de politiques de sécurité tout en leur assurant un contrôle d'accès réseau complet (NAC). Fiables et simples à utiliser, nos produits protègent plus de 100 millions d'utilisateurs dans plus de 150 pays. Nos 20 ans d'expérience et notre réseau international de centres d'analyse des menaces nous permettent de répondre rapidement aux menaces émergentes et d'atteindre les niveaux de satisfaction clientèle les plus élevés du secteur. Sophos est une société internationale siégeant à Boston aux Etats-Unis et à Oxford au Royaume-Uni.

Boston, USA • Mayence, Allemagne • Milan, Italie • Oxford, RU • Paris, France
Singapour • Sydney, Australie • Vancouver, Canada • Yokohama, Japon

© Copyright 2007. Sophos Plc. Tous droits réservés. Toutes les autres marques appartiennent à leurs propriétaires respectifs.
ds/070405

SOPHOS
secured.