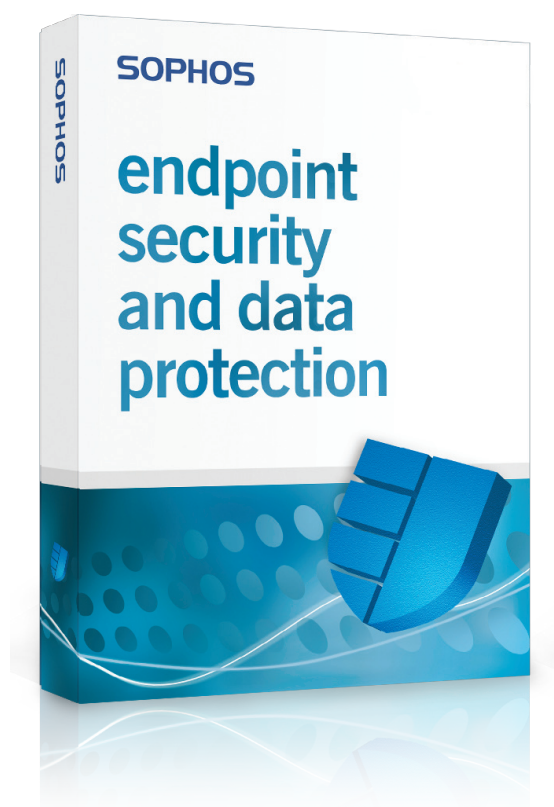


Guide d'évaluation

# Sophos Endpoint Security and Data Protection

**SOPHOS**





## BIENVENUE

Ce document détaille les principaux composants logiciels de Sophos Endpoint Security and Data Protection, la solution de sécurité totalement intégrée et adaptable pour systèmes d'extrémité. Ce document présente tous les éléments logiciels clés de Sophos Endpoint Security and Data Protection : console d'administration, antivirus, pare-feu client, contrôle des données, contrôle des périphériques, contrôle des applications et contrôle de l'accès réseau

Ce guide présente les puissantes fonctionnalités de Sophos Endpoint Security and Data Protection. Après l'avoir lu, vous comprendrez mieux comment Sophos Endpoint Security and Data Protection assure dans l'entreprise la protection la plus fiable et la plus rentable qui soit contre les menaces connues et inconnues et contre les fuites de données. Cette solution permet de se concentrer sur d'autres tâches importantes pour une meilleure continuité et efficacité de l'entreprise et des systèmes.

Pour plus d'informations sur les tarifs et l'acquisition de Sophos Endpoint Security and Data Protection, contactez votre interlocuteur Sophos le plus proche. Pour connaître le représentant de votre région, consultez la page :

[www.sophos.fr/companyinfo/contacting](http://www.sophos.fr/companyinfo/contacting)

Si vous désirez demander une évaluation, connectez-vous à :

<http://www.sophos.fr/products/enterprise/free-trials/endpoint>

La documentation concernant l'installation est accessible à l'adresse suivante :

[www.sophos.fr/support/docs](http://www.sophos.fr/support/docs)

## SOMMAIRE

<b>1 PROTECTION COMPLETE DES SYSTEMES D'EXTREME</b>	<b>5</b>
Présentation de Sophos Endpoint Security and Data Protection	
<b>2 UNE CONSOLE UNIQUE, AUTOMATISÉE ET CENTRALISÉE</b>	<b>8</b>
Présentation de Sophos Enterprise Console	
<b>3 PROTECTION DES ORDINATEURS</b>	<b>24</b>
Présentation de Sophos Endpoint Security and Control, Sophos Client Firewall, Sophos NAC et SafeGuard Disk Encryption	
<b>4 PROTECTION DES ORDINATEURS NON WINDOWS</b>	<b>30</b>
Présentation de Sophos Anti-Virus pour Mac OS X, Linux et UNIX	

## ANNEXES

<b>I ÉVALUATION D'ENDPOINT SECURITY AND DATA PROTECTION</b>	<b>33</b>
Suggestion de réseau de test	
<b>II LE VIRUS TEST EICAR</b>	<b>36</b>
<b>III AUTRES PRODUITS ET SERVICES SOPHOS</b>	<b>37</b>

SOPHOS ENDPOINT SECURITY AND DATA PROTECTION

## 1 PROTECTION COMPLETE DES SYSTEMES D'EXTREMITE

### PRÉSENTATION DE SOPHOS ENDPOINT SECURITY AND DATA PROTECTION

Sophos simplifie la sécurisation de vos postes de travail, portables, périphériques mobiles et serveurs de fichiers face aux menaces connues et inconnues et protège votre entreprise contre les fuites accidentelles de données.

#### Sécurité intégrale

Le client antivirus unifié de Sophos évite d'avoir plusieurs produits pour bloquer différentes menaces. En un seul contrôle, vous protégez votre entreprise contre les virus, spywares, adwares, rootkits et applications potentiellement indésirables (PUA). Vous pouvez contrôler simultanément l'installation et l'utilisation des logiciels non autorisés tels que le VoIP (Voix sur IP), les messageries instantanées (MI) et le partage de fichiers en peer-to-peer (P2P), contrôler l'utilisation des périphériques de stockage amovibles et les protocoles de réseau sans fil et surveiller le transfert des informations sensibles. Vous pouvez également protéger vos données contre les pertes éventuelles via le chiffrement complet des disques de vos ordinateurs et des données sur vos périphériques amovibles, et sécuriser ainsi l'échange de données avec les tierces parties.

#### Une console simplifiée et automatisée

La console automatisée de Sophos, l'Enterprise Console, constitue le point central à partir duquel vous pouvez déployer et mettre à jour la solution sur l'ensemble de votre parc informatique et éditer les rapports de protection. Grâce à une seule et même console, vous administrez des dizaines de milliers d'ordinateurs Windows, Mac, Linux et UNIX. Cette protection simplifiée et automatisée permet de réduire les coûts, de réaliser toutes les tâches en quelques clics seulement et de bénéficier d'une meilleure visibilité du réseau. En outre, l'administration déléguée vous permet de partager les tâches avec d'autres utilisateurs afin de réduire la charge de travail, tout en gardant le contrôle des politiques de sécurité au sein de votre parc informatique.

#### Une solution pour toutes vos plates-formes

Lorsque vous achetez une licence Endpoint Security and Data Protection, vous disposez d'un logiciel qui protège plus de 25 plate-formes (l'éventail le plus large que puisse vous proposer un éditeur), y compris Windows, Mac OS X, Linux, UNIX, NetWare, NetApp Storage Systems et Windows Mobile.

## Des données parfaitement sécurisées

Sophos a combiné différentes technologies pour garantir la protection de vos données contre les pertes accidentelles. Le contrôle du contenu intégré dans un seul agent garantit que toutes les données sensibles qui sont transférées par les utilisateurs vers les périphériques de stockage amovibles et les applications Internet telles que les messageries de courriers électroniques et les messageries instantanées sont détectées et peuvent être analysées. Le contrôle précis des périphériques de stockage amovibles permet l'autorisation de périphériques spécifiques, la mise en place de périphériques chiffrés ou même l'accès en lecture seule. Et le chiffrement intégral du disque dur sécurise les données sur ordinateurs, empêchant les informations de tomber dans de "mauvaises mains" en cas de perte d'ordinateurs.

## Une expertise complète

Grâce au savoir-faire des SophosLabs™ en matière de malwares, de spam et de protection web, vous bénéficiez à coup sûr d'une protection plus rapide et plus efficace. Combinées aux mises à jour de signatures rapides, des technologies uniques comme Behavioral Genotype® Protection bloquent les malwares nouveaux et inconnus et assurent régulièrement la supériorité de Sophos sur Symantec et McAfee.



## Conformité des systèmes d'extrémité

Sophos Endpoint Security and Data Protection offre une fonction de protection préventive qui fait appel à Sophos NAC pour évaluer et contrôler tous les systèmes d'extrémité. Sophos NAC vérifie que l'antivirus et les autres applications de sécurité sont bien actifs et à jour et contrôle que les systèmes d'exploitation disposent bien des correctifs et mises à jour nécessaires. Le risque d'infection par un malware est ainsi réduit : les ordinateurs vulnérables sont mis en quarantaine et corrigés avant même qu'ils puissent accéder au réseau. Sophos NAC continue de protéger la session utilisateur avec des vérifications périodiques.

Raisons	Avantages de Sophos
Editeur fiable	Bénéficiant de plus de 20 ans d'expérience dans la protection contre les menaces connues et inconnues, nous répondons rapidement aux menaces émergentes, quelle que soit leur complexité.
Une approche plus simple et plus intelligente	La Sophos Enterprise Console permet une administration économique, centralisée et intuitive à travers des plates-formes multiples, offrant une visibilité et un contrôle hors pair sur l'ensemble de votre réseau.
Une excellente réactivité	En analysant continuellement les nouveaux malwares et en fournissant rapidement des mises à jour de petite taille, les experts des SophosLabs veillent en permanence sur les nouvelles menaces.
Une qualité de support inégalée	Disponible 24 heures sur 24, 365 jours par an et inclus dans le prix de la licence, le support technique Sophos est assuré à plein temps par une équipe locale de spécialistes disposant d'un savoir-faire extrêmement pointu qui nous permet d'atteindre le plus haut niveau de satisfaction client du marché.
Un système simplifié de licence	Une licence par abonnement unique garantit les mises à jour et les mises à niveaux gratuites, régulières et automatiques à chaque nouvelle version et l'assistance technique 24h/24 et 7j/7, et ce sans aucun coût caché.
Une offre centrée sur les entreprises	En vendant uniquement ses produits aux professionnels, Sophos focalise ses activités d'ingénierie, d'assistance et de recherche sur les besoins des entreprises sans essayer de s'adresser également aux particuliers.

Tableau 1 : Pourquoi les clients font confiance à Sophos

## Vérification des principales fonctions

Avant de tester nos produits, voici quelques éléments qu'il peut être utile de prendre en compte et de comparer avec la concurrence :

- Pouvez-vous gérer la protection de tous vos systèmes à partir d'une seule et même console d'administration ?
- Combien de déploiements sont nécessaires pour offrir une protection identique des systèmes d'extrémité regroupant antivirus, antispyware, pare-feu, analyse comportementale HIPS, contrôle des applications et contrôle d'accès réseau ?
- Quel est le niveau de simplicité de l'installation et du déploiement du produit dans l'entreprise ? Pouvez-vous utiliser Active Directory (AD) pour accélérer la procédure ?
- Une synchronisation avec AD est-elle possible afin de permettre un déploiement automatique de la protection sur les ordinateurs rejoignant le réseau ?
- Est-il simple d'évaluer et de contrôler l'accès réseau des ordinateurs gérés et non gérés ?
- La console d'administration offre-t-elle un tableau de bord en temps réel regroupant les états et les alertes ?
- Le produit est-il simple à administrer ? En particulier, quelle est la durée nécessaire à l'accomplissement de tâches d'administration courantes telles que la modification de stratégies et leur application à des groupes, et combien d'étapes sont nécessaires ?
- Quel est le niveau d'efficacité des technologies de détection proactive et d'analyse HIPS et combien d'opérations de configuration sont nécessaires pour activer et maintenir une protection efficace ?
- L'agent peut-il contrôler le transfert des données sensibles vers les périphériques de stockage amovibles et les applications Internet telles que les courriels, les navigateurs web et les messageries instantanées ?
- Est-il facile de contrôler l'utilisation des périphériques de stockage amovibles et quelles sont les différentes options disponibles ?
- Est-il facile d'empêcher les utilisateurs de télécharger et d'installer des applications légitimes que vous ne souhaitez pas voir utilisées sur le réseau d'entreprise, telles que les applications de messagerie instantanée, de P2P, de voix sur IP et les jeux ? Est-il compliqué de maintenir les listes d'applications à jour avec les nouvelles versions ?
- Quelle est la quantité de mémoire accaparée par le client ? Les mises à jour de protection sont-elles volumineuses et quelle est leur fréquence ?
- Pouvez-vous bénéficier d'un service d'assistance composé de spécialistes expérimentés, géographiquement proches et disponibles sans frais supplémentaires 24 heures sur 24, 7 jours sur 7 ?

## 2 UNE SEULE CONSOLE AUTOMATISEE ET CENTRALISEE

### PRÉSENTATION DE SOPHOS ENTERPRISE CONSOLE

Sophos Enterprise Console permet d'administrer la protection de vos systèmes par la mise en place de politiques de manière simplifiée et intelligente. Vous pouvez ainsi administrer des milliers d'utilisateurs Windows, Mac, Linux et UNIX à partir d'une même console.

La simplicité d'administration de la console et d'exploitation des stratégies sur l'intégralité du réseau et le nettoyage centralisé et ciblé réduisent considérablement les coûts de gestion récurrents.

Trop élaborées, de nombreuses solutions de sécurité sont un fardeau pour l'administrateur qui doit gérer des systèmes de plus en plus complexes. L'Enterprise Console a été conçue pour offrir une approche simple et intégrée qui permet de réagir rapidement face aux problèmes émergents. Cette section met en avant les fonctionnalités clés de l'Enterprise Console et détaille ses avantages uniques.

### UN SEUL DÉPLOIEMENT SUFFIT

#### Protection des systèmes et suppression des logiciels tiers

Endpoint Security and Data Protection permet de déployer et d'administrer l'antivirus, le pare-feu client et la fonction de contrôle d'accès réseau sur tous les systèmes d'extrémité à partir d'une unique console.

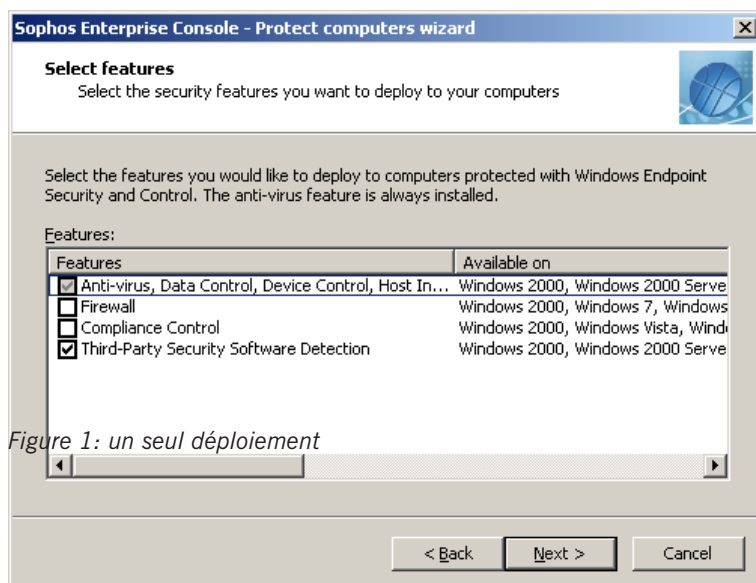


Figure 1: un seul déploiement

La migration vers Endpoint Security and Data Protection à partir de votre solution existante s'en trouve accélérée et vous disposez en plus d'une option permettant de désinstaller les logiciels de sécurité des autres éditeurs au cours du déploiement.

## INTÉGRATION ET SYNCHRONISATION ACTIVE DIRECTORY

### Déploiement plus rapide et protection automatique

Sophos Endpoint Security and Data Protection facilite la détection des ordinateurs de votre réseau en permettant la réplication des groupes Active Directory et de la structure cliente dans Enterprise Console.

Une fois la réplication réalisée, vous pouvez synchroniser Active Directory avec Enterprise Console afin que toutes les modifications effectuées dans Active Directory soient automatiquement répercutées dans Enterprise Console. Ainsi, les nouveaux clients rejoignant le réseau sont automatiquement protégés. Par défaut, Enterprise Console vérifie automatiquement toutes les heures les modifications apportées dans Active Directory.

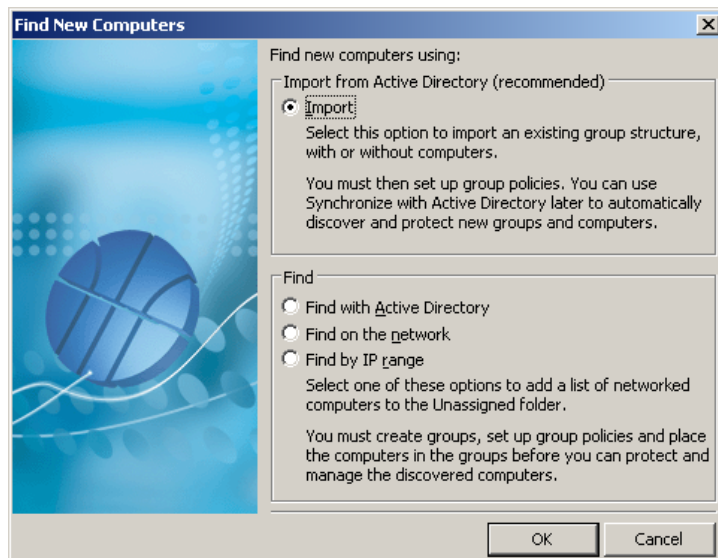


Figure 2 : Recherche rapide de nouveaux ordinateurs

Si vous n'utilisez pas Active Directory, vous disposez de deux autres méthodes pour identifier rapidement les ordinateurs :

- utilisation de la détection réseau intégrée
- recherche par plage IP/de sous-réseau.

## TABLEAU DE BORD DE SÉCURITÉ

### Meilleure visibilité et système d'alerte automatique

Lorsqu'un virus, un spyware, un adware, une application potentiellement indésirables ou tout élément suspect est détecté, une alerte est automatiquement générée et affichée sur le tableau de bord.

Les niveaux de risque d'épidémies virales sur l'ensemble du réseau sont affichés sur le tableau de bord de sécurité d'Enterprise Console. Ce tableau réunit les alertes provenant des ordinateurs Windows, Mac et Linux et utilise le code couleur suivant : bleu pour le statut OK, orange pour Avertissement ou rouge pour Critique.

D'un simple clic de souris, vous pouvez :

- Filtrer la vue pour vous concentrer sur les ordinateurs avec une protection obsolète ou avec une alerte de malware, ou pour un aperçu instantané des zones de votre réseau qui réclament votre attention.
- Régler dans le tableau de bord les seuils à partir desquels la couleur des statuts doit changer.
- Activer l'envoi automatique d'alertes par courriel lorsque les seuils de sécurité définis sont sur le point d'être atteints.

Grâce à ces fonctionnalités, il n'est pas nécessaire d'ouvrir une session sur la console pour être alerté de tout problème de sécurité potentiel.

Par défaut, des alertes apparaissent sur le bureau de tout ordinateur sur lequel un malware, une PUA ou une application non autorisée a été détecté. Des alertes par courriel et des alertes SNMP peuvent également vous être envoyées ou être envoyées à des utilisateurs spécifiques lorsque des virus, des applications potentiellement indésirables ou des erreurs sont détectés sur un des ordinateurs du groupe. Tous les virus détectés sur l'ordinateur apparaîtront avec un lien hypertexte menant à leur entrée correspondante dans la bibliothèque de virus du site web de Sophos.

### Suivi des évènements critiques

Lorsqu'un événement relatif au contrôle des applications, au pare-feu, au contrôle des données ou au contrôle des périphériques est repéré sur un système (par exemple une application ayant été bloquée par le pare-feu), celui-ci est envoyé à l'Enterprise Console et s'affiche dans l'observateur d'événements.

### Tableau de bord ergonomique

La possibilité de visualisation immédiate des zones présentant un problème est un immense avantage. Des alertes sont envoyées automatiquement par courriel si les seuils de sécurité sont dépassés.

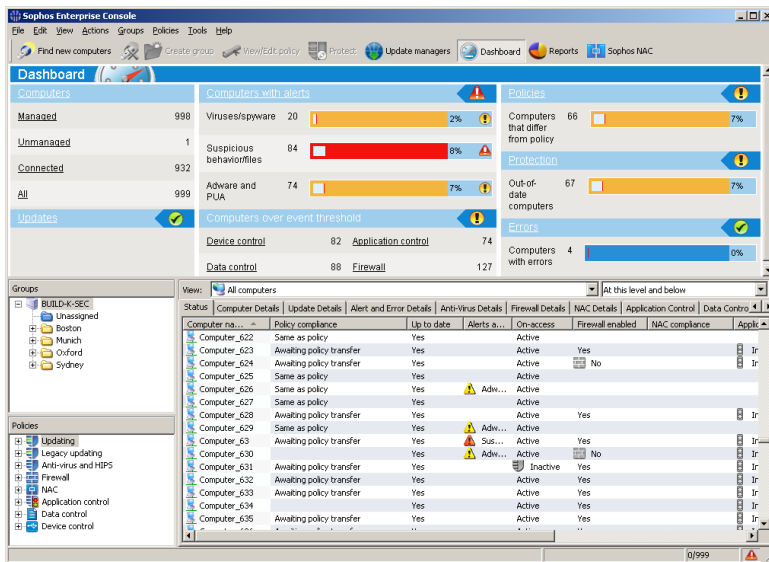


Figure 3 : Tableau de bord de sécurité de la Sophos Enterprise Console

Grâce à l'observateur d'événements, vous pouvez rapidement et facilement rechercher les événements qui sont survenus sur le réseau. Vous pouvez également générer une liste d'événements basé sur un filtrage que vous avez configuré, par exemple, une liste de tous les événements de contrôle des données pour un utilisateur spécifique lors des sept derniers jours.

Les ordinateurs présentant un nombre d'événements dépassant un seuil spécifique au cours des sept derniers jours s'affiche sur le tableau de bord. Vous pouvez également programmer l'envoi d'alertes à une sélection de destinataires lorsqu'un événement survient.

## SMART VIEWS

### Nettoyage ciblé

Le nettoyage d'un vaste réseau après une attaque peut s'avérer extrêmement long et coûteux. L'Enterprise Console permet le nettoyage centralisé et distant des fichiers, entrées de registre et processus en cours d'exécution. Smart Views offre une vue complète de l'état de la sécurité de tous les ordinateurs du réseau dans une seule et même console. Vous pouvez ainsi choisir d'afficher uniquement les ordinateurs réclamant une attention particulière et une correction, par exemple ceux dont la protection n'est pas à jour ou ceux qui ne respectent pas la politique.

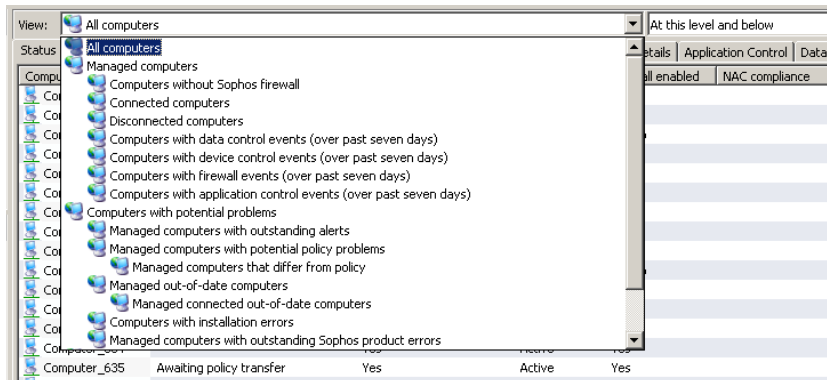


Figure 4 : Smart Views

## SOPHOS UPDATE MANAGER

### Des mises à jour rapides gérées depuis un point unique

Le Sophos Update Manager garantit que votre réseau est protégé en permanence grâce aux mises à jour automatiques de votre logiciel de sécurité depuis Sophos. Un gestionnaire de mise à jour est installé et administré avec l'Enterprise Console.

Une fois que vous avez configuré un gestionnaire de mise à jour, celui-ci :

- Se connecte à intervalles réguliers à la banque de distribution des données de Sophos et de votre réseau.
- Télécharge les mises à jour nécessaires pour le logiciel de sécurité auquel l'administrateur est abonné.
- Place le logiciel mis à jour sur un ou plusieurs réseaux pour l'installer sur les systèmes d'extrémité.

Les systèmes d'extrémité se mettent ensuite à jour automatiquement à partir des partages de réseau, conformément à la politique de mises à jour que vous avez configurée.

## ACTIVEPOLICIES

### Configuration et application des politiques simplifiées

Grâce à Sophos ActivePolicies™, vous pouvez créer et déployer rapidement et intuitivement sur tout le réseau des politiques de sécurité indépendamment des groupes, ce qui permet de déployer une politique simultanément sur plusieurs groupes. ActivePolicies facilite l'application des politiques de sécurité dans sept domaines essentiels.

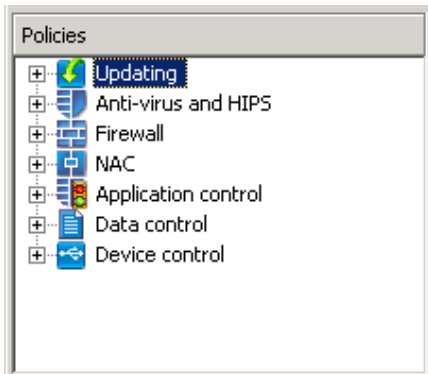


Figure 5 : ActivePolicies

#### Politiques de mises à jour

L'Enterprise Console vous permet de maintenir vos postes à jour avec la protection la plus récente. Vous pouvez configurer les heures auxquelles les différentes parties du réseau se mettent à jour et les emplacements auxquels les ordinateurs se connectent pour leurs mises à jour. Cette fonction est très utile si, dans votre entreprise, plusieurs réseaux couvrent différents fuseaux horaires ou si vos employés utilisent leurs postes à des moments différents, surtout des portables distants se connectant au réseau. Le contrôle des paramètres de mise à jour automatique vous permet aussi de minimiser l'effet des mises à jour sur les performances de votre réseau.

La configuration des paramètres d'abonnement au logiciel permet de spécifier quelles versions des logiciels sont téléchargées de Sophos pour chaque plate-forme. L'abonnement par défaut comprend le dernier logiciel pour Windows 2000 et versions supérieures.

Vous pouvez aussi resserrer la bande passante pour empêcher les ordinateurs de l'employer intégralement pour les mises à jour alors qu'elle peut être utile pour d'autres tâches comme le téléchargement.

### Politiques antivirus et HIPS

En installant notre solution antivirus, vous installez aussi un système complet de prévention des intrusions sur l'hôte (HIPS), et ce, sans configuration complexe nécessaire. Des opérations d'analyse runtime, de détection des dépassements de la mémoire tampon et de protection exclusive avant exécution sont réalisées, pour une détection proactive des malwares, des fichiers et des comportements suspects.

Cette stratégie vous permet de configurer pour tout le réseau un large éventail d'options de contrôle. Vous pouvez configurer les contrôles sur accès, planifiés et à la demande et choisir d'exclure certains types de fichiers là où vous savez qu'ils ne constituent aucune menace. Les ordinateurs utilisent par défaut la politique de sécurité suivante :

- Contrôle de tous les fichiers vulnérables aux malwares.
- Refus d'accès à tout fichier contenant un virus, spyware, etc.
- Apparition d'une alerte sur le bureau de tout ordinateur sur lequel un virus ou une PUA a été détecté.

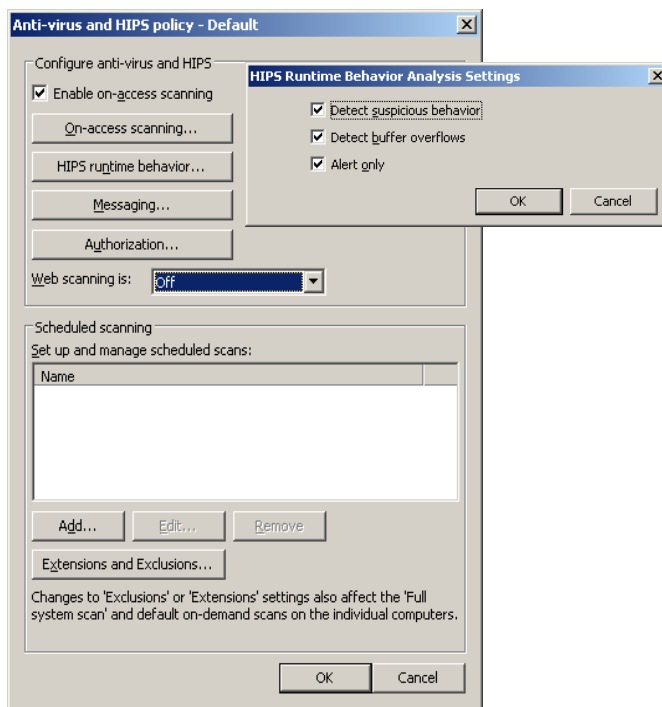


Figure 6 : Configurer la politique anti-virus et HIPS

### Politiques de contrôle des applications

Les logiciels de voix sur IP, de messagerie instantanée et les applications P2P posent de plus en plus de problèmes de sécurité, juridiques et de productivité à l'entreprise, obligeant les services informatiques à contrôler leur installation et leur usage. Sophos intègre la détection de ces applications contrôlées mais aussi des malwares et des PUA, permettant ainsi un contrôle sans qu'il soit utile de se procurer, d'installer ou de gérer un produit distinct.

Toutes les applications contrôlées sont par défaut autorisées, mais vous pouvez utiliser l'Enterprise Console pour configurer des politiques par groupes d'ordinateurs afin de refléter les besoins en sécurité des différents sites ou départements. Par exemple, il est possible de désactiver une application de voix sur IP sur les ordinateurs de l'entreprise mais de l'autoriser sur les ordinateurs distants. Pour bloquer une application, il vous suffit de la déplacer dans la colonne des applications bloquées.

La liste des applications contrôlées est fournie par Sophos et mise à jour régulièrement. Vous ne pouvez pas ajouter de nouvelles applications à la liste mais vous pouvez soumettre une requête à Sophos pour inclure une nouvelle application légitime que vous voudriez contrôler sur votre réseau.

Pour une liste complète des applications que vous pouvez contrôler, consultez notre site à la page :

<http://www.sophos.fr/security/analyses/controlled-applications/>

### Les applications pouvant être contrôlées sont les suivantes :

- Voix sur IP
  - Messagerie instantanée
  - Logiciel peer-to-peer
  - Projets informatiques distribués
  - Barres d'outils de moteur de recherche
  - Lecteurs multimédia
  - Navigateurs Internet
  - Jeux (Windows et jeux multijoueur)
  - Applications de virtualisation
  - Outils d'administration à distance
  - Applications de cartographie
  - Clients de messagerie
- Stockage en ligne  
Outils de chiffrement

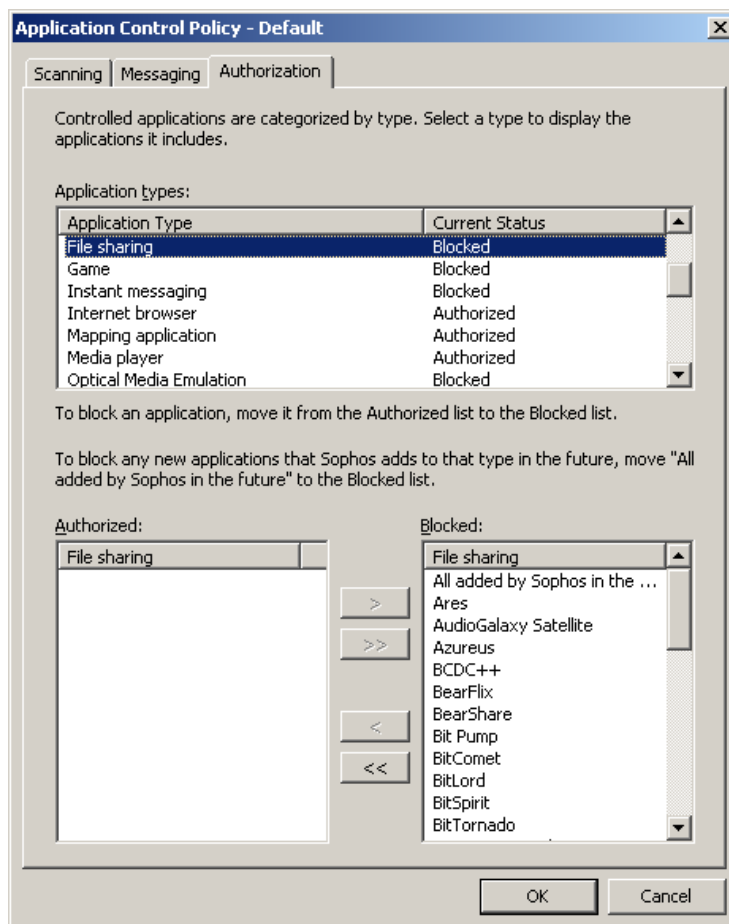


Figure 7 : Contrôle des applications - contrôle simplifié des logiciels non autorisés

### Politiques des contrôles de périphériques

Le contrôle des périphériques vous aide à réduire de manière significative votre exposition aux pertes de données accidentelles et à limiter la possibilité des utilisateurs à introduire des logiciels et des malwares dans votre environnement réseau.

Intégré à l'agent Sophos, il permet de contrôler trois types de périphériques :

- Stockage : les périphériques de stockage amovibles (clés USB, lecteurs de cartes PC et disques durs externes) ; lecteurs de supports (CD-ROM/DVD/Blu-ray) ; lecteurs de disquettes ; périphériques de stockage amovibles sécurisés
- Réseau : Modems ; Sans fil (Interfaces Wi-Fi , norme 802.11)
- Faible portée : Interfaces Bluetooth ; Infrarouge (interfaces IrDA)

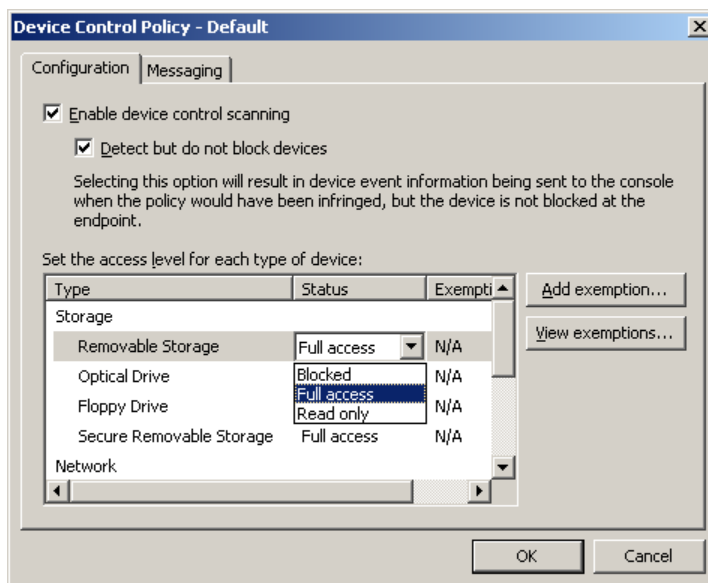


Figure 8 : Contrôle des périphériques – Contrôle précis des périphériques de stockage amovibles

Par défaut, le contrôle des périphériques est désactivé et tous les périphériques sont autorisés. Si vous souhaitez activer la fonction de contrôle des périphériques pour la première fois, Sophos vous recommande de :

- Sélectionner les types de périphériques que vous souhaitez contrôler.
- Détecter les périphériques sans les bloquer.
- Utiliser les rapports du contrôle des périphériques pour décider ceux qui doivent être bloqués et ceux qui doivent être autorisés.
- Détecter puis bloquer ou autoriser les périphériques pour un accès aux périphériques en lecture seule.

Chaque type de périphérique prend en charge à la fois les instances de périphériques et les modèles d'exception. Cela signifie qu'une clé USB qui appartient au département IT peut être exemptée de la politique de blocage des périphériques de stockage amovibles.

La gestion des exceptions est facilitée via l'observateur d'événements sur le contrôle des périphériques dans la Sophos Enterprise Console. Elle permet de filtrer et de vérifier rapidement les événements générés par la politique de contrôle des périphériques et d'autoriser les périphériques en les exemptant de la politique.

Vous pouvez également réduire de manière significative les risques de ponts réseaux entre le réseau professionnel et le réseau non professionnel. Le mode Block Bridged est disponible à la fois pour les modems et les périphériques sans fil. Ce mode fonctionne en désactivant les adaptateurs réseau modem ou sans fil lorsqu'un système d'extrémité est connecté à un réseau physique (habituellement via une connexion Ethernet). Une fois que le système d'extrémité est déconnecté du réseau physique, les adaptateurs réseau ou sans fil sont réactivés sans problème.

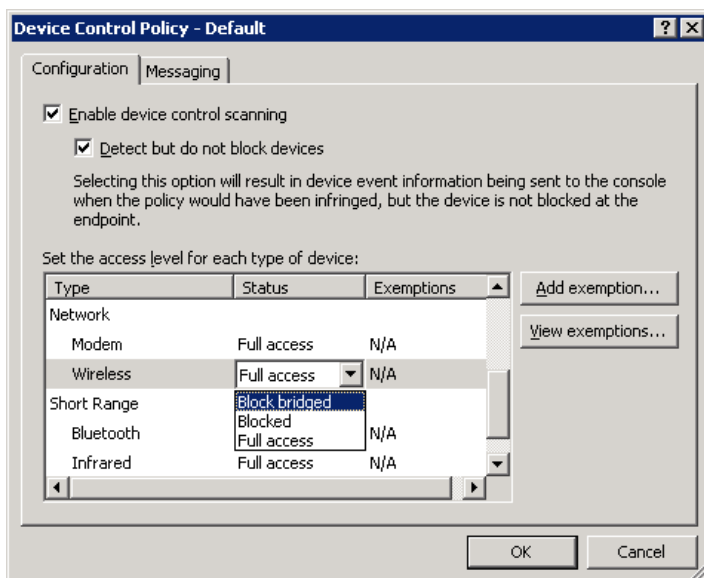


Figure 9 : Contrôle des périphériques – Prévention des ponts

### Politiques de contrôle des données

Déployer une solution de DLP autonome pour protéger contre la perte accidentelle de données sensibles peut nécessiter beaucoup de temps et d'argent, et peut avoir un impact significatif sur les performances du système de vos systèmes. Sophos facilite la tâche en intégrant le contrôle des données sensibles à l'agent du système, simplifiant ainsi la configuration, le déploiement et l'administration.

Vous pouvez surveiller et contrôler le transfert des fichiers vers des périphériques de stockage spécifiés (par ex. des supports de stockage amovibles ou des lecteurs optiques) ou vers des applications Internet spécifiques (par ex. client email, navigateur Web ou messageries instantanées) sans avoir à déployer une solution spécifique and un autre agent.

Sophos propose plusieurs options de règles pré-définies pour le contrôle des données, couvrant entre autres les numéros d'identification nationale, les indicateurs de documents confidentiels, etc. Vous pouvez utiliser ces règles telles quelles ou les adapter en fonction de vos besoins.

Il existe deux types de règles de contrôle des données :

- règle de correspondance de fichiers : spécifie l'action à prendre si l'utilisateur tente de transférer un fichier avec le nom de fichier ou le type de fichier spécifiés (catégorie du type de fichier véritable, par ex. une feuille de calcul) vers la destination spécifique. Par exemple, blocage du transfert des bases de données vers les périphériques de stockage amovibles
- règle de contenu : contient une ou plusieurs définitions des données et spécifie l'action à prendre si l'utilisateur tente de transférer des données qui correspondent aux définitions définies dans la règle de destination spécifiée.

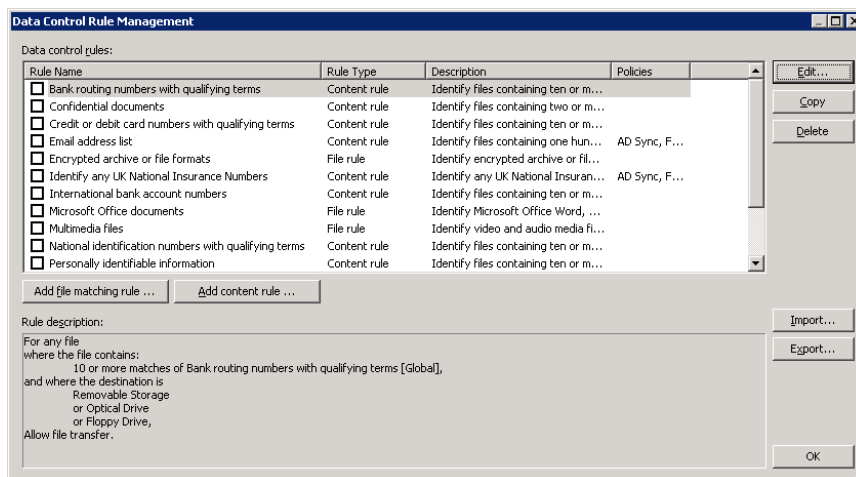


Figure 10 : Contrôle des données – règles de politiques préconfigurées

Pour simplifier la création des politiques, les SophosLabs maintiennent une bibliothèque étendue de définitions de données sensibles internationales (Content Control Lists) qui couvrent les informations personnelles identifiables (PII) telles que les numéros de cartes de crédit, les numéros de sécurité sociales, les adresses postales ou les adresses électroniques.

Ces définitions utilisent un large éventail de techniques pour garantir un très haut niveau de détection. Elles sont revues en permanence par les SophosLabs et les nouvelles définitions sont ajoutées lors des mises à jour mensuelles.

Vous pouvez créer vos propres listes propres à votre organisation telles que les numéros de référence client ou les Indicateurs de document confidentiel.

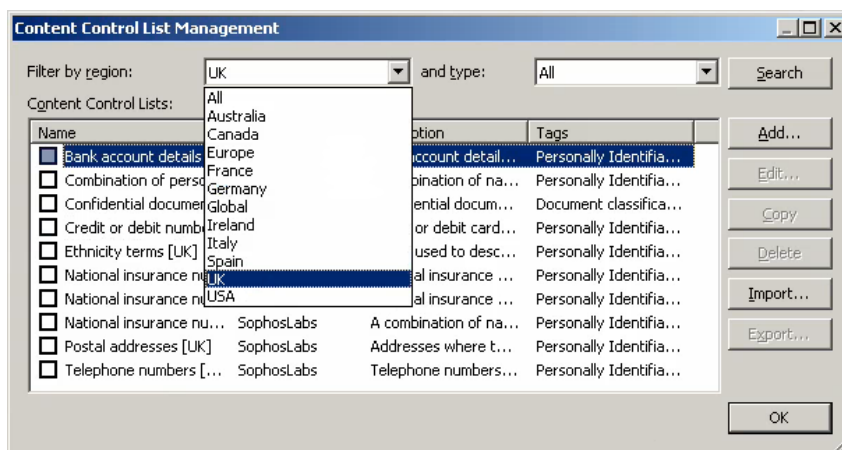


Figure 11 : Contrôle des données – Listes de contrôle du contenu

Il existe un certain nombre d'actions qui peuvent être prises lorsqu'une règle de contrôle de données s'applique :

- Autoriser le transfert de fichiers et le journal des événements
- Autoriser le transfert sur acceptation par l'utilisateur et le journal des événements
- Bloquer le transfert et le journal des événements

Par défaut, lorsqu'une règle s'applique et le transfert de fichiers est bloqué ou la confirmation de l'utilisateur pour le transfert du fichier est requise, un message s'affiche sur l'ordinateur (bureau) du système d'extrémité. Vous pouvez facilement ajouter vos propres messages personnalisés aux messages standards pour demander aux utilisateurs la confirmation ou le blocage du transfert des fichiers.

L'action « autoriser le transfert sur acceptation de l'utilisateur » peut être utilisée pour informer les utilisateurs que les données qu'ils sont en train de transférer peuvent aller à l'encontre de la politique de l'entreprise sans pour autant bloquer le transfert. La décision des utilisateurs finaux est audité et peut être revue ultérieurement.

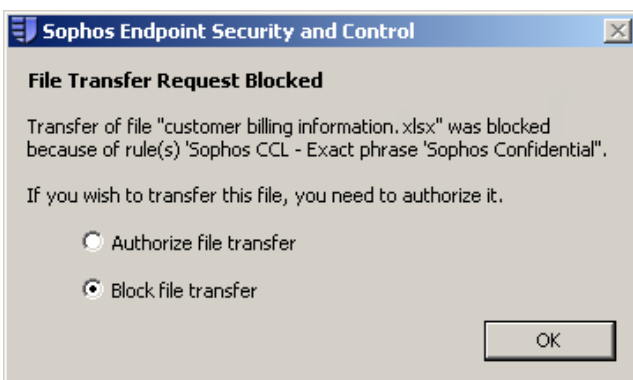


Figure 12 : Contrôle des données – Notification d'autorisation de l'utilisateur

Lorsqu'un événement de contrôle des données survient, par exemple, la copie d'un fichier contenant des données sensibles vers un support de stockage USB, l'événement est envoyé à l'Enterprise Console et peut être visualisé dans l'observateur d'événements sur le contrôle des données. Le nombre d'ordinateurs ayant enregistré des événements sur une période donnée au cours des sept derniers jours s'affichera également sur le tableau de bord.

### Politiques de pare-feu

Par défaut, Sophos Client Firewall est activé sur tous les ordinateurs de tous les groupes et bloque tout trafic non indispensable. Sophos Client Firewall dispose de plusieurs politiques de sécurité par défaut que vous pouvez modifier facilement pour les adapter à vos besoins. Toutes les options de configuration du pare-feu peuvent être administrées de manière centralisée (consultez la section 3 pour plus d'informations sur Sophos Client Firewall).

Le mode “Alert seulement” permet de déployer le pare-feu sur l'ensemble du parc informatique pour collecter des informations sur toutes les applications qui sont utilisées sur le réseau. Ces informations sont renvoyées à la console et vous pouvez les utiliser pour mettre au point la politique qui n'aura pas d'impact sur la productivité des utilisateurs, avant de déployer une politique “live”.

Vous pouvez configurer différentes politiques de sécurité variables en fonction de l'emplacement du système ("location awareness") pour garantir que les ordinateurs portables soient protégés, aussi bien dans l'entreprise qu'à l'extérieur. L'emplacement de l'ordinateur portable est détecté en utilisant le DNS ou l'adresse MAC de la passerelle.

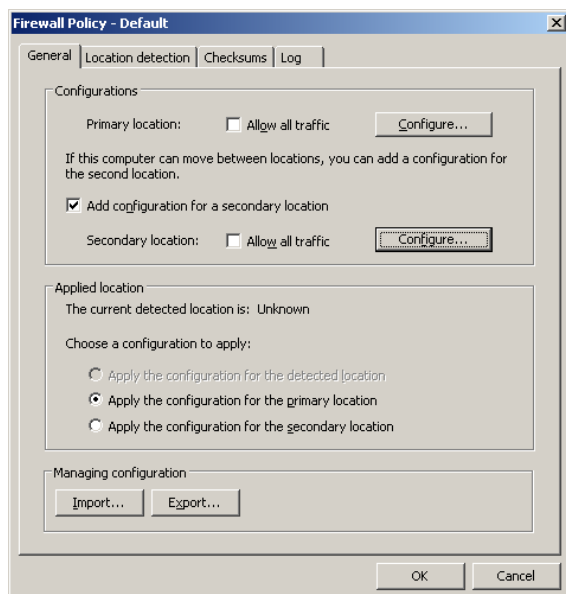


Figure 13 : Pare-feu variable en fonction de l'emplacement du système

### Politiques de contrôle d'accès réseau

Les stratégies de contrôle d'accès réseau peuvent être contrôlées grâce à l'application NAC Manager, accessible à partir du bouton du menu NAC qui se trouve en haut de la console ou par un double-clic sur une politique de contrôle d'accès réseau.

Endpoint Security and Data Protection propose des politiques prédéfinies conçues pour les ordinateurs gérés et non gérés. NAC Manager dispose de nombreuses options de modification des politiques, d'édition de rapports, d'envoi d'alertes, de contrôle d'accès et de configuration des systèmes, réparties dans quatre zones de fonctions : administration, application, rapports et configuration.

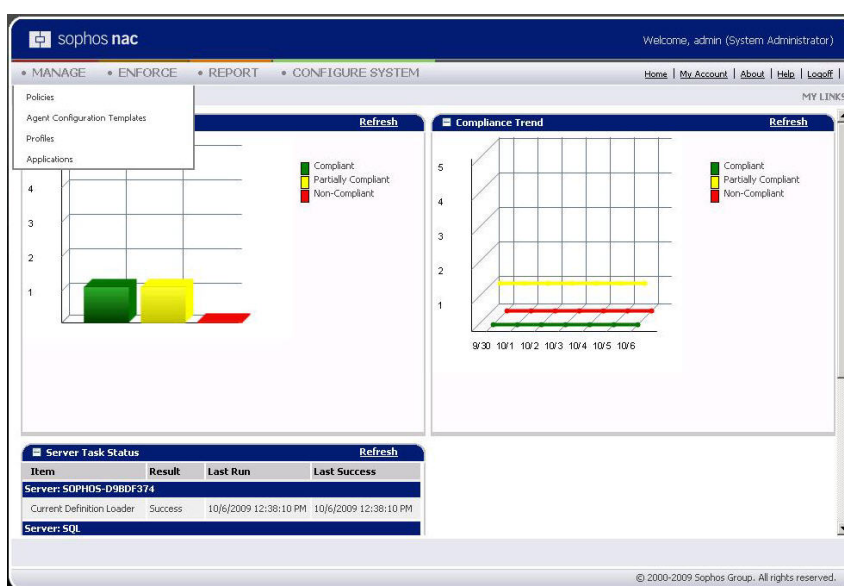


Figure 14 : L'interface d'administration NAC offre un aperçu en temps réel de la conformité sur l'ensemble du réseau

- Administration : offre différents composants permettant de modifier les stratégies et d'administrer ces mêmes stratégies ainsi que les ordinateurs.
- Application : permet de contrôler l'accès réseau par le biais de modèles d'accès et d'exceptions.
- Rapports : permet de créer différents rapports destinés à régler les problèmes de conformité et d'accès réseau.
- Configuration : offre différents composants permettant d'administrer et de configurer les systèmes et le serveur.

Une fois connecté, vous disposez d'un aperçu en temps réel de la conformité générale de votre entreprise. Le diagramme de conformité actuelle indique en temps réel combien d'ordinateurs du réseau respectent la politique de sécurité et combien la respectent partiellement ou sont considérés comme non conformes. Un autre diagramme illustre les tendances de conformité récentes.

### Des stratégies prédéfinies pour les ordinateurs gérés et non gérés

Les stratégies permettent de contrôler l'accès de groupes spécifiques aux ressources du réseau en fonction de l'évaluation de la sécurité de l'ordinateur de chaque utilisateur. Elles déterminent également l'état de conformité de l'ordinateur, les messages affichés, les mesures correctives réalisées et les mesures d'application mises en place.

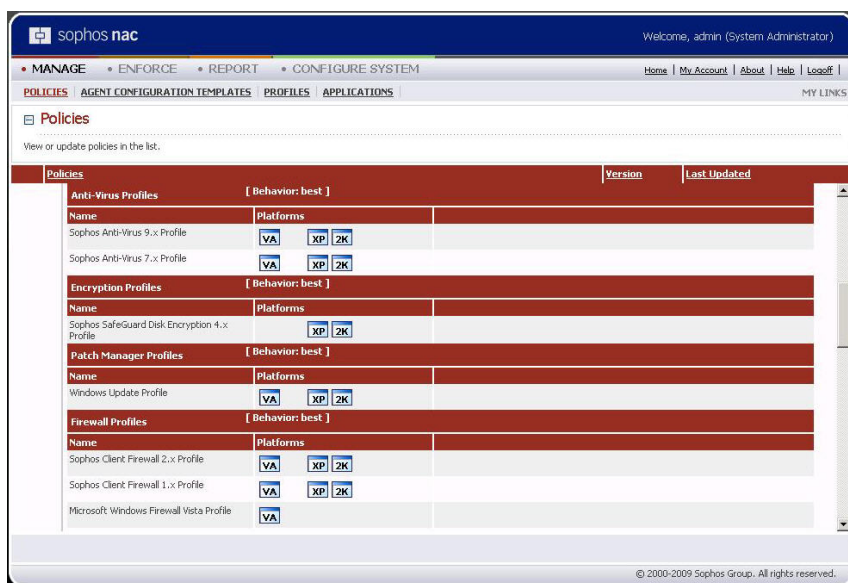


Figure 15 : Politiques pré-configurées permettant de vérifier la conformité des ordinateurs

Il existe trois stratégies de contrôle d'accès réseau prédéfinies :

- Par défaut : la politique par défaut est conçue pour permettre d'accéder aux clients gérés et de les contrôler rapidement. Tous les nouveaux groupes Enterprise Console et les clients auxquels aucune politique n'est appliquée, ainsi que les clients dont la politique est introuvable, seront associés à la politique par défaut. Cette politique par défaut est préconfigurée avec Sophos Anti-Virus, Sophos SafeGuard Encryption, Sophos Client Firewall, Microsoft/Windows Update et MS Windows Firewall XP SP2/Vista.
- **Administré** — La politique administrée est identique à la politique par défaut. Elle permet d'apporter des modifications à l'une de ces stratégies et de la tester avant de l'appliquer à tous les ordinateurs.
- Non gérée : cette politique est appliquée aux ordinateurs qui rejoignent temporairement le réseau et qui sont évalués par l'agent Web. Elle est préconfigurée pour évaluer différents produits de sécurité dont les antispywares, antivirus et pare-feu les plus répandus, ainsi que Windows ou Microsoft Update. Elle évalue notamment les produits Sophos, Microsoft, Trend Micro, McAfee, Symantec/Norton, F-Secure, Panda, Spybot et Ad-Aware.

### Important

Pour évaluer l'ensemble des fonctions de Sophos NAC, téléchargez et installez le composant de gestion de contrôle d'accès réseau à partir de la page [www.sophos.fr/downloads/](http://www.sophos.fr/downloads/) (vos identifiants d'évaluation vous seront demandés pour l'accès à cette zone).

## RELAIS DE MESSAGES

### Une évolutivité remarquable

Sophos Endpoint Security and Data Protection a été conçu pour permettre une évolutivité remarquable afin que vous puissiez administrer des dizaines de milliers d'ordinateurs à partir d'une seule et même console. Cette évolutivité est renforcée par les relais de messages, permettant aux ordinateurs du réseau de jouer le rôle de relais pour Enterprise Console. Cette fonction réduit le trafic et la charge du réseau sur le serveur d'administration et permet aux grands comptes de gérer des dizaines de milliers d'ordinateurs.

## RAPPORTS

### Edition de rapports personnalisés et planifiés

Pour le maintien de la sécurité, l'édition intégrée et à la demande de rapports est cruciale. L'Enterprise Console propose un nombre de rapports avec données textuelles et graphiques sur plusieurs aspects du statut de sécurité de votre réseau. Ils peuvent être utilisés tels quels ou être facilement configurés pour répondre à vos besoins. Les rapports standards incluent :

- Alertes par élément
- Alertes par emplacement
- Alertes par heure
- Historique des alertes
- Résumé des alertes
- Non conformité à la politique
- Protection administrée des systèmes
- Hiérarchie des mises à jour
- Événements par utilisateur

Vous pouvez afficher les rapports sous la forme d'un tableau ou d'un graphique (par ex. circulaire) et les exporter dans un certain nombre de formats de fichiers : PDF (Acrobat), HTML, MS Excel, MS Word, RTF, CSV, XML.

Grâce au Report Manager, vous pouvez créer en toute simplicité un rapport basé sur le modèle actuel, changer la configuration d'un rapport existant et programmer l'édition d'un rapport à un moment déterminé et à une fréquence régulière (quotidienne, hebdomadaire, mensuelle) puis paramétrer l'envoi automatique des résultats à un groupe de destinataires prédéfinis.

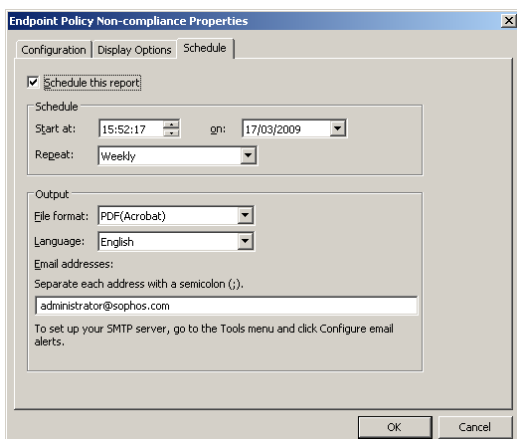


Figure 16 : programmation des rapports

Les autres fonctions d'édition de rapports permettent d'afficher des informations sur des ordinateurs spécifiques. Un double-clic sur le nom d'un ordinateur affiche une boîte de dialogue offrant différentes informations telles que l'adresse IP, le nom d'utilisateur et la dernière date de contrôle.

## ADMINISTRATION DELEGUEE

### Administration déléguée pour alléger la charge de travail

La possibilité de configurer des rôles, des droits d'administration et des sous-parcs confère une grande souplesse pour administrer la sécurité sur l'ensemble du parc informatique.

Vous pouvez configurer l'accès à l'Enterprise Console de manière à partager l'administration avec des équipes et des individus spécifiques, en utilisant les rôles pré-configurés ou en créant vos propres rôles. Par exemple, un ingénieur du Service d'aide pourra mettre à jour ou nettoyer les postes de travail mais ne pourra pas configurer les politiques, qui est de la responsabilité de l'administrateur.

Pour configurer l'accès, il vous suffit de créer les rôles nécessaires, ajouter des droits spécifiques puis les assigner aux utilisateurs et aux groupes Windows.

Quatre rôles pré-configurés sont proposés :

**Administrateur système** — Rôle préconfiguré qui possède tous les droits pour administrer le logiciel de sécurité Sophos sur le réseau et les rôles dans l'Enterprise Console. Le rôle Administrateur Système ne peut pas être modifié ni supprimé.

**Administrateur** — Rôle préconfiguré qui possède les droits pour administrer le logiciel de sécurité Sophos sur le réseau mais ne peut pas administrer les rôles dans l'Enterprise Console. Le rôle Administrateur peut être renommé, modifié ou supprimé.

**Service d'aide**— Rôle préconfiguré qui possède les droits de correction seulement, par exemple nettoyer ou mettre à jour les ordinateurs. Le rôle Service d'aide peut être renommé, modifié ou supprimé.

**Invité** — Rôle préconfiguré qui peut uniquement accéder à l'Enterprise Console en lecture seule. Le rôle Invité peut être renommé, modifié ou supprimé.



Figure 17 : Gérer l'administration déléguée

### Administration des sous-parcs

En divisant votre parc informatique en sous-parcs, vous pouvez également limiter les ordinateurs et les groupes sur lesquels les utilisateurs effectuent des opérations.

Vous pouvez contrôler l'accès aux sous-parcs en leur attribuant les utilisateurs et les groupes Windows. Un utilisateur pourra voir uniquement les groupes et les postes appartenant à son sous-parc.

Les rapports sont également spécifiques au sous-parc. Les politiques ne seront applicables que dans le sous-parc pour lesquelles elles ont été créées. Un administrateur ne peut pas changer les politiques qui s'appliquent hors de leur sous-parc.

Pour l'édition de rapports, les administrateurs peuvent seulement configurer et éditer des rapports applicables à leur propre sous-parc. Un administrateur système pourra exécuter des rapports sur l'ensemble du parc informatique.

## STOCKAGE DES INFORMATIONS ÉVOLUTIF

### Intégration de Microsoft SQL Server

L'Enterprise Console est intégrée en standard dans MSDE (Microsoft SQL Server Desktop Engine) pour stocker des informations de gestion. Si vous êtes dans une grande entreprise, il peut être intéressant d'utiliser Microsoft SQL Server car ses fonctionnalités ont été fortement améliorées et son adaptabilité aux vastes réseaux est plus grande.

## SOPHOS ENDPOINT SECURITY AND DATA PROTECTION

## 3 PROTECTION DES ORDINATEURS WINDOWS

Sophos Endpoint Security and Data Protection protège votre réseau Windows par le biais de Sophos Anti-Virus, Sophos Client Firewall, SafeGuard Disk Encryption et Sophos NAC.

## SOPHOS ENDPOINT SECURITY AND CONTROL POUR WINDOWS

Conçu pour les réseaux d'entreprise, Sophos Anti-Virus offre plus qu'une simple protection contre les malwares en incorporant un système de prévention des intrusions sur l'hôte (HIPS) et un contrôle des applications non autorisées et des périphériques de stockage amovibles.

L'agent unique élimine le besoin de recourir à plusieurs produits autonomes, pour offrir :

- Anti-virus et HIPS (bloque les virus, les spywares, les adwares, les PUA et les fichiers et comportements suspects.)
- Contrôle des applications (empêche l'installation et l'utilisation des applications non autorisées)
- Contrôle des périphériques (administre l'utilisation des périphériques de stockage amovibles et des protocoles de réseau sans fil)
- Contrôle des données (contrôle le transfert des données sensibles depuis le système d'extrémité)
- Pare-feu client (protège contre les pirates et les communications entre applications non autorisées)

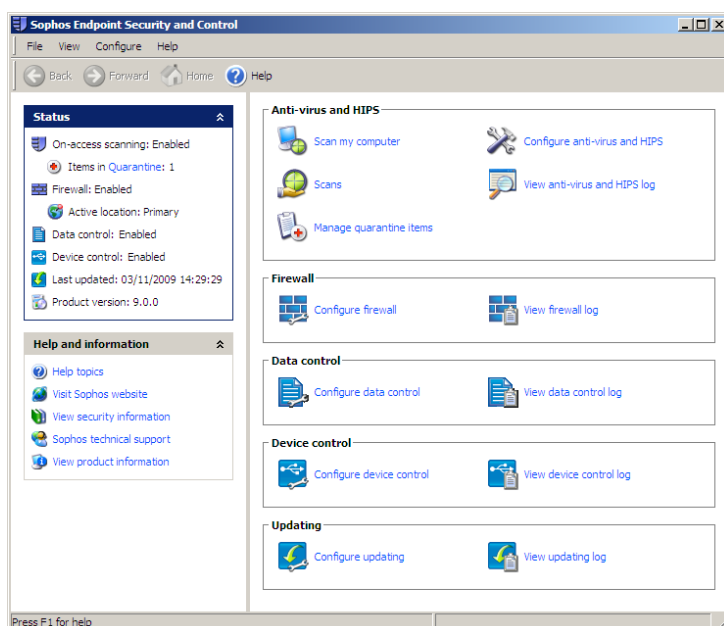


Figure 18 : L'agent unique diminue significativement l'impact sur les performances du système

## Prévention des intrusions

Sophos Endpoint Security intègre un système complet de prévention des intrusions sur l'hôte (HIPS) offrant une protection proactive sans pour autant nécessiter l'installation ou la configuration d'un produit distinct complexe. Un certain nombre de technologies de détection préemptives sont associées pour protéger votre réseau contre les menaces mixtes et ciblées du jour zéro.

- **La technologie Genotype®** assure une protection du jour zéro en reconnaissant les familles et variantes de virus connus et en permettant leur blocage préemptif avant même qu'une détection spécifique ne soit disponible.
- **La technologie Behavioral Genotype®** Protection protège automatiquement votre infrastructure contre les menaces nouvelles et ciblées en analysant leur comportement avant l'exécution du code.
- **Les technologies intégrées de prévention des intrusions sur l'hôte** comprenant détection de fichiers suspects avant leur exécution, analyse des comportements suspects et runtime et protection contre les dépassements de mémoire tampon sont réunis pour détecter malwares, fichiers et comportements suspects.

## Analyse accélérée grâce à la technologie Decision Caching

Decision Caching™, la technologie de contrôle sur accès hautes performances de Sophos Anti-Virus pour Windows, optimise les performances en ne procédant au contrôle que des fichiers nouveaux ou modifiés. De plus, la technologie de reconnaissance intelligente des fichiers signifie que seuls ceux susceptibles de contenir des malwares sont contrôlés. Avant de se reconnecter au réseau principal, l'utilisateur distant peut effectuer des contrôles à la demande de fichiers individuels ou de son ordinateur, offrant ainsi une couche de sécurité supplémentaire.

## Gestionnaire de quarantaine

Le gestionnaire de quarantaine permet de déplacer ou de supprimer les fichiers infectés et de bloquer un par un les PUA et les applications contrôlées.

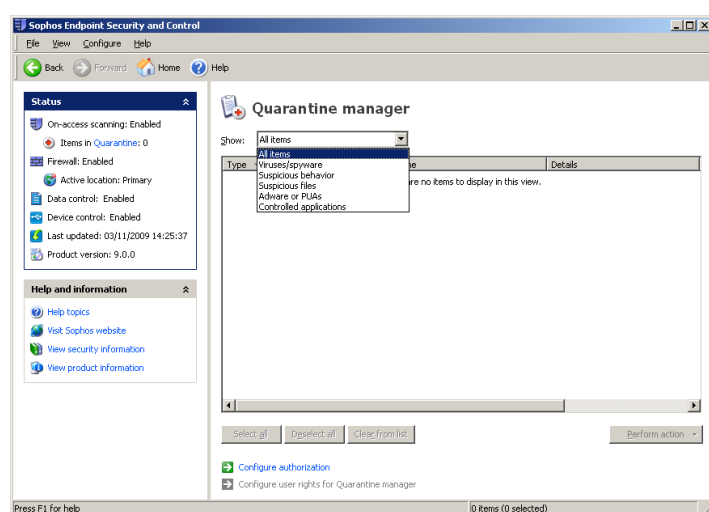


Figure 19 : Gestionnaire de quarantaine

## Contrôle des applications

Si certaines applications améliorent la productivité, d'autres empêchent l'utilisateur de se consacrer pleinement à son travail et gaspillent la bande passante du réseau et les ressources de traitement. Par ailleurs, avec le développement rapide des attaques de malwares par P2P ou messagerie instantanée et la mise en place de réglementations obligeant les entreprises à assurer la pérennité et la protection de leurs données, il est de plus en plus essentiel de contrôler l'installation des applications non autorisées.

Sophos a intégré le contrôle des applications à son agent pour système d'extrémité, en vous laissant autoriser ou bloquer une à une les applications au niveau du poste de travail ou de manière centralisée. À l'aide du composant ActivePolicies de Sophos Enterprise Console (voir chapitre 2), vous pouvez également bloquer ou autoriser les applications pour différents groupes d'ordinateurs. Ainsi, vous pouvez bloquer les logiciels de voix sur IP sur les postes de travail locaux tout en les autorisant sur les ordinateurs distants.

## Contrôle des périphériques

Notre technologie de contrôle des périphériques réduit les risques de fuites de données et d'infection par des malwares, en vous donnant le contrôle sur les périphériques de stockage amovibles et les protocoles de réseau sans fil.

Intégré à l'agent unique, il prend en charge tous les ports utilisés pour connecter le périphérique, et notamment les interfaces USB, FireWire, SATA et PCMA.

Initialement, la politique de contrôle des périphériques peut être appliquée en mode notification uniquement, pour vous permettre d'avoir une visibilité sur l'utilisation des périphériques au sein de votre parc informatique sans bloquer aucun périphérique, avant de configurer et de déployer la politique de contrôle aux groupes correspondants.

Chaque type de périphérique peut soit être autorisé (paramétrage par défaut) soit bloqué. Les périphériques de stockage peuvent être paramétrés en mode "lecture seule", ce qui signifie qu'il est possible de lire les données sur un périphérique mais pas d'enregistrer. Cela peut être très utile pour les clés USB et les lecteurs de CD/DVD.

Pour les interfaces réseau, le mode "Block bridging" empêche les ponts réseaux et désactivera l'interface sans fil de l'ordinateur si celui-ci possède une connexion physique au réseau, par ex. un câble Ethernet. Une fois que le câble est déconnecté, l'interface sans fil sera activée.

## Contrôle des données

Sophos est le premier fournisseur à intégrer le contrôle de contenu DLP à l'agent, réduisant l'impact sur les performances du système avec un agent unique qui contrôle les données sensibles ainsi que les malwares et qui facilite la configuration, le déploiement et l'administration.

Il vous permet de détecter si les utilisateurs transfèrent des données sensibles, telles que les informations personnelles identifiables (PII) ou des documents confidentiels professionnels vers des périphériques de stockage amovibles ou des applications Internet, vous aidant ainsi à prévenir les pertes accidentelles de données.

La configuration des politiques est simplifiée grâce à une série de règles de contrôle de données préconfigurées, pouvant être utilisées telles quelles ou adaptées à vos besoins.

Les SophosLabs maintiennent également une bibliothèque étendue de définitions de données sensibles internationales (Content Control Lists) qui couvrent les informations personnelles identifiables (PII) telles que les numéros de cartes de crédit, les numéros de sécurité sociales, les adresses postales ou encore les adresses email, vous aidant à protéger vos données sensibles plus rapidement.

Vous pouvez créer vos propres listes, s'appliquant à votre organisation telles que les numéros de référence client ou les indicateurs de documents confidentiels.

## SOPHOS NAC

### Évaluez et contrôlez tous les systèmes d'extrémité Windows

Lorsqu'un ordinateur essaie de se connecter au réseau, Sophos NAC évalue sa conformité par rapport à une politique de sécurité définie. Cette fonction de conformité permet également de garantir que tous les ordinateurs sont correctement protégés grâce aux éléments suivants :

- Vérification de l'activation et des mises à jour des antivirus et autres applications de sécurité
- Vérification de la mise à jour des Service Pack du système d'exploitation Microsoft Windows
- Vérification de l'activation de Windows Update et/ou de Microsoft Update
- Politiques distinctes pouvant être configurées pour les ordinateurs gérés, les ordinateurs de sous-traitants et les ordinateurs invités

### Options d'application du contrôle d'accès réseau

Sophos NAC fait appel à des agents pour appliquer le contrôle des ordinateurs gérés et à Microsoft DHCP pour empêcher les ordinateurs non gérés ou non autorisés d'accéder au réseau. L'évaluation des systèmes est effectué par :

- l'agent Sophos NAC installé sous forme de résident sur le client
- L'agent Sophos NAC Compliance Dissolvable (Composant Java téléchargeable)

L'agent Sophos NAC installé, dont le déploiement s'effectue dans Sophos Enterprise Console, permet d'évaluer et de contrôler les ordinateurs gérés avant et pendant une session réseau, selon un intervalle que vous pouvez définir vous-même. Grâce à cet agent, les ordinateurs non conformes se mettent automatiquement en quarantaine.

L'agent Web Sophos NAC réalise cette même évaluation avant que les ordinateurs non gérés présents sur le réseau local puissent accéder au réseau. Il est conçu pour les utilisateurs qui ne disposent pas d'agent installé sur leur système et qui ont besoin d'accéder aux ressources réseau spécifiques, telles que les sous-traitants ou les invités. Il utilise Microsoft DHCP pour protéger le réseau vis-à-vis des ordinateurs connectés au réseau local en s'appuyant sur l'infrastructure Microsoft DHCP existante de l'entreprise, ce qui permet à Sophos NAC de mettre en quarantaine les ordinateurs non conformes et non autorisés.

## SOPHOS CLIENT FIREWALL

Sophos Client Firewall est intégré à l'agent système, simplifiant ainsi le déploiement, la configuration, la mise à jour et l'administration via l'Enterprise Console. Il verrouille les ordinateurs de manière proactive pour assurer une protection contre les menaces connues et inconnues comme les vers Internet, les pirates et les applications non autorisées. Grâce à des fonctions qui empêchent le piratage et l'usurpation des applications, Sophos Client Firewall assure une protection supérieure aux simples pare-feu bloquant les ports offerts par la plupart des éditeurs de sécurité.

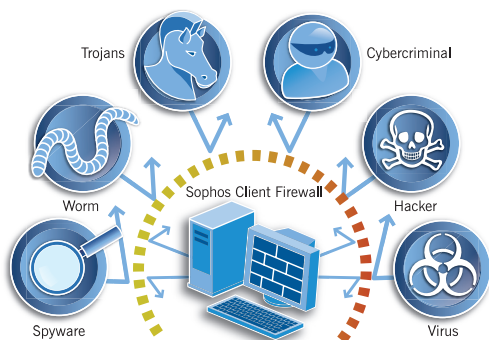


Figure 20 : Protection du jour zéro

### Protection du jour zéro contre les menaces connues et inconnues

Sophos Client Firewall fonctionne de pair avec Sophos Anti-Virus® pour assurer une protection du jour zéro, comblant la vulnérabilité existante entre l'émergence d'une nouvelle menace et le déploiement d'une protection. Il protège tous les ordinateurs de l'entreprise contre les menaces complexes et à propagation rapide et empêche les irrptions avant qu'elles ne perturbent l'activité de l'entreprise.

### Verrouillage proactif

Sophos Client Firewall assure une protection contre les vers de réseau et Internet, les pirates et les risques de connexion au réseau des ordinateurs non protégés en verrouillant de manière proactive ceux en interne mais aussi les portables se connectant via des points d'accès sans fil ou des connexions ADSL.

### Surveillance et blocage des ports pour éliminer les menaces

Sophos Client Firewall bloque les menaces connues et inconnues en surveillant les ports actifs et en fermant tous les ports inactifs, bloquant ainsi les vers Internet et les pirates.

### Mode furtif – blocage des intrusions par les pirates

Les cybercriminels comme les pirates informatiques se servent du contrôle des ports pour identifier et cibler les ordinateurs vulnérables avec des ports ouverts. Ils envoient pour cela des demandes de connexion sur Internet. Le mode furtif de Sophos empêche l'ordinateur de répondre à ces demandes en le masquant et en le rendant inactif pour le monde extérieur. En ôtant toute chance à ses pirates d'identifier et de cibler les ordinateurs protégés, vous disposez ainsi d'un niveau supplémentaire de protection garantissant votre confidentialité.

## Une protection intuitive garantie selon les connexions

Sophos Client Firewall vous permet de configurer les différentes politiques pour les différents emplacements en fonction de l'endroit où les ordinateurs sont utilisés, par exemple dans l'entreprise (sur le réseau) ou à l'extérieur. L'Enterprise Console applique alors les différents paramètres de pare-feu aux ordinateurs, selon s'ils se trouvent sur le réseau ou pas. Cette double configuration s'avère très importante pour les postes mobiles tels que les ordinateurs portables.

## Empêcher le piratage et l'usurpation des applications

Le filtrage des applications sert à surveiller leur comportement et à autoriser seulement l'accès Internet ou réseau à celles correspondant à vos spécifications. Sophos Client Firewall empêche le piratage des applications en surveillant les appels d'applications ou système inappropriés et le lancement des processus cachés. Il utilise par ailleurs la technique des sommes de contrôle pour déjouer les tentatives des spywares et autres malwares de passer pour des applications légitimes, empêchant ainsi le vol d'informations confidentielles par Internet.

## Contrôle par inspection dynamique des paquets de données entrants et sortants

Pour une sécurité renforcée, Sophos Client Firewall utilise l'inspection dynamique en suivant à la trace les paquets de communications et en veillant à ce que seuls les paquets légitimes accèdent au réseau. Le suivi des paquets permet de limiter les communications de réponse. Par exemple, si un paquet sortant est envoyé, alors seuls les paquets entrants générés par l'ordinateur qui a reçu la communication (via le port approprié) sont autorisés via le pare-feu.

## Centralisation de l'édition des rapports et de la journalisation

Le pare-feu envoie un rapport centralisé à la console d'administration. Ce rapport inclut les applications et le trafic inconnus, les processus camouflés et les événements mémoire modifiés. Toutes ces informations vous permettent de déceler les zones à risque pour votre sécurité. D'autre part, la visionneuse de journaux du pare-feu permet de voir, de filtrer et d'enregistrer les détails des connexions autorisées ou bloquées par le pare-feu.

## Mode Moniteur uniquement

Le pare-feu peut être déployé sur l'ensemble de votre parc informatique en mode "alerte seulement". Il détectera toutes les applications qui sont utilisées sur le réseau (en prenant en compte les paramètres LAN que vous avez effectués). Les résultats sont rapportés dans l'Enterprise Console. Cela permet de recueillir des informations sur le trafic inconnu, pour vous permettre de redéfinir les politiques de manière rapide, sans impact sur la productivité.

## Fonctionnement interactif

Le pare-feu peut s'exécuter en mode apprentissage (interactif), et demande alors à l'utilisateur comment gérer le trafic détecté. Si ce mode est activé, le pare-feu affiche une fenêtre à chaque fois qu'une application ou un service inconnus demandent à accéder au réseau. La boîte de dialogue propose à l'utilisateur plusieurs options : autoriser le trafic, bloquer le trafic ou créer une règle pour ce type de trafic.

## 4 PROTECTION DES ORDINATEURS NON WINDOWS

### LES ORDINATEURS NON WINDOWS DOIVENT AUSSI ÊTRE PROTÉGÉS

Il devient de plus en plus nécessaire de protéger les ordinateurs Mac, Linux, UNIX et autres. L'éventualité que des ordinateurs non-Windows hébergent et diffusent des virus Windows, l'apparition occasionnelle de virus ciblés Mac et Linux et les demandes juridiques de protection de tous les ordinateurs, tout cela est de plus en plus lourd à supporter pour l'utilisateur.

Sophos Anti-Virus pour Mac OS X, Sophos Anti-Virus pour Linux et Sophos Anti-Virus pour UNIX offrent une solution puissante et intuitive pour les serveurs, postes de travail et portables d'extrémité.

### SOPHOS ANTI-VIRUS POUR MAC OS X

Sophos Anti-Virus pour Mac OS X détecte en temps réel et à la demande virus, spywares, chevaux de Troie et vers et nettoie automatiquement les malwares Windows et Mac. Sophos Anti-Virus pour Mac OS X détecte également les virus contenus dans les pièces jointes compressées, y compris les archives récursives.

### Administration depuis Mac ou Windows

Sophos Anti-Virus pour Mac peut être administré depuis Sophos Update Manager pour Mac ou la Sophos Enterprise Console (Windows). Vous n'avez pas besoin d'exécuter ces deux interfaces administrateur pour garantir que Sophos Anti-Virus pour Mac OS X est maintenu à jour.

### Administration centralisée

L'Enterprise Console permet de configurer et d'administrer de manière centralisée la protection antimalware des ordinateurs Windows, Mac, Linux et UNIX sur l'ensemble du réseau. Elle ne nécessite pas la présence d'un poste Windows et offre une fonction d'administration renforcée.

Si vous disposez d'un réseau Mac uniquement, Sophos Update Manager pour Mac permet la mise à jour et la configuration depuis un simple ordinateur Mac. Cette application permet de configurer les mises à jour automatiques et la manière dont vous souhaitez recevoir les notifications par courriel. Elle permet aussi de configurer le déroulement des contrôles sur les postes de travail et les ordinateurs portables, et offre la possibilité de configurer de manière centralisée les paramètres des postes de travail.

### Mises à jour automatiques proposées par les SophosLabs

Vous pouvez utiliser la Sophos Enterprise Console ou la Sophos Update Manager pour Mac OS X pour gérer les mises à jour de la protection et du logiciel.

Pour mettre à jour les ordinateurs et installer les fichiers d'identités virales (IDE) les plus récents proposés par les SophosLabs, il vous suffit d'indiquer l'adresse, le nom d'utilisateur et le mot de passe nécessaires. Vous pouvez aussi paramétrer les ordinateurs pour qu'ils se mettent à jour depuis le répertoire d'installation centralisée, configuré sur le réseau pendant le processus d'installation.

Vous pouvez également autoriser les utilisateurs distants et mobiles à procéder à une mise à jour via le réseau ou Internet, où qu'ils se trouvent, à partir du serveur principal, d'une sauvegarde ou directement auprès de Sophos.

### Édition automatique de rapports sur les incidents viraux

Le tableau de bord d'Enterprise Console signale les risques d'irruptions. Des alertes automatiques par courriel sont envoyées en cas d'irruption afin que vous puissiez prendre le plus tôt possible les mesures appropriées.

Grâce à Sophos Update Manager pour Mac, vous pouvez définir des options d'alerte pour le contrôle immédiat et les résultats du contrôle sur accès. Naturellement, vous pouvez sélectionner le destinataire du message. Si l'expéditeur n'est pas connecté, les alertes sont stockées et sont transférées lorsqu'il se reconnecte au réseau pour éviter toute perte.

### Réduction des montées en charge lors des contrôles

Sophos Anti-Virus contrôle les fichiers sur accès et à la demande, reconnaît intelligemment les types de fichiers non infectables et permet ainsi d'économiser des ressources système.

Dans Sophos Update Manager, vous pouvez configurer un certain nombre d'options de contrôle, permettant notamment d'exclure certains fichiers du contrôle, et définir les actions à privilégier en cas de détection d'une menace (désinfection ou suppression, par exemple).

## SOPHOS ANTI-VIRUS POUR LINUX

Sophos Anti-Virus pour Linux offre un contrôle sur accès supérieur pour les postes de travail, portables et serveurs Linux. Très performant, stable et fiable, ce logiciel prêt à l'emploi s'adapte à un grand éventail de distributions Linux.

### Administration centralisée

Les ordinateurs Linux peuvent être administrés par l'Enterprise Console. Le tableau de sécurité indique les niveaux de risque d'épidémies virales et des alertes automatiques sont envoyées par courriel lorsque les seuils de sécurité de votre choix sont menacés. Chaque incident viral est automatiquement signalé, facilitant ainsi l'administration quotidienne.

### Déploiement rapide sur les réseaux Linux seulement

Red Hat Package Manager peut être utilisé pour le déploiement dans les environnement Linux seulement ; la configuration et la mise à jour peuvent être effectuées à distance par l'intermédiaire d'une interface utilisateur de type web ou d'une interface par lignes de commande.

### Performances, stabilité et fiabilité assurées

Talpa, le module d'interception de fichiers de Sophos, assure une protection très performante en permettant les contrôles sur accès, à la demande et planifié des disques durs locaux, des lecteurs multimédia, des systèmes de fichiers communs (comme NFS et Samba) et des systèmes de gestion DFS. Un très grand nombre de noyaux Linux sont pris en charge immédiatement, y compris des versions 64 bits récentes. Pour une protection optimale, vous pouvez ainsi changer de version, effectuer des mises à niveau et en compiler si besoin est.

## Mises à jour automatiques

Les mises à jour sont automatiquement téléchargées et distribuées via l'Enterprise Console, les serveurs web en cascades ou directement depuis Sophos, pour une protection de tous les ordinateurs du réseau, y compris les portables à distance.

## SOPHOS ANTI-VIRUS POUR UNIX

Sophos Anti-Virus pour UNIX assure une détection antivirus et antispyware intégrée et multi plates-formes sur les serveurs, postes de travail et ordinateurs portables UNIX. Le puissant moteur de détection virale de Sophos contrôle tous les points d'entrée potentiels pour une protection totale du réseau.

## Souplesse de gestion

Sophos Anti-Virus pour UNIX peut être administré par ligne de commande ou via l'Enterprise Console (pour Solaris 9 et 10 sur SPARC et Intel (i386), vous offrant la souplesse dont vous avez besoin.

## Contrôle hautes performances

Les opérations de contrôle et de désinfection peuvent être réalisées à la demande ou automatiquement à des heures planifiées, pour un impact minime sur les performances du système. Grâce à la technologie Decision Caching™, seuls les fichiers modifiés sont à nouveau contrôlés. Le contrôle est ainsi plus rapide et ne pèse que très peu sur les performances du système.

## Détection des menaces du jour zéro avant leur exécution

Notre technologie Behavioral Genotype® Protection assure une protection automatique contre les menaces inconnues en analysant leur comportement avant que leur code ne s'exécute. Elle propose ainsi tous les avantages d'un système de prévention des intrusions sur l'hôte (HIPS).

## Édition automatique de rapports personnalisés

Chaque incident viral est automatiquement signalé à l'administrateur pour une administration quotidienne facilitée.

## ANNEXE I

# EVALUER SOPHOS ENDPOINT SECURITY AND DATA PROTECTION

Nous tenons à vous convaincre que Sophos Endpoint Security and Data Protection protégera votre réseau mieux que les produits proposés par les autres éditeurs de solutions de sécurité. Cet annexe vous donne des détails sur la documentation dont vous aurez besoin pour évaluer nos logiciels, suggère un réseau de test et vous propose une liste de contrôle complète pour vous aider à considérer chaque aspect du logiciel et du support technique que nous offrons.

### Guide de démarrage et manuels utilisateur

Avant de procéder à l'évaluation de Sophos Endpoint Security and Data Protection, téléchargez le guide de démarrage réseau. Pour cela, connectez-vous à :

[http://www.sophos.fr/support/docs/Endpoint\\_Security\\_Control-all.html](http://www.sophos.fr/support/docs/Endpoint_Security_Control-all.html)

### RÉSEAU DE TEST

Sophos Anti-Virus est pris en charge sur de nombreuses plates-formes, y compris UNIX, Linux et NetWare. En revanche, pour évaluer les fonctions d'administration centralisée de l'Enterprise Console, vous aurez besoin d'au moins un ordinateur Windows. Nous vous suggérons d'avoir les éléments suivants dans votre réseau de test :

- Une console d'administration, c'est-à-dire un ordinateur fonctionnant sous Windows 2000/XP/2003.
- Au moins un client. Nous vous recommandons d'utiliser un poste de travail Windows 2000/XP/2003/Vista/7.

Vous aurez par ailleurs besoin d'accéder à Internet. Si vous le souhaitez, vous pouvez également inclure dans votre réseau de test des systèmes Mac OS X, Linux et UNIX ainsi qu'un poste autonome distant, et ce, afin d'évaluer les fonctions de mise à jour et de configuration à distance.

### Important

Si un autre antivirus est installé sur votre réseau de test, commencez par le désinstaller. Si cette opération pose problème, contactez le support technique de Sophos. Les coordonnées sont disponibles à l'adresse suivante : [www.sophos.fr/support/queries](http://www.sophos.fr/support/queries)

## CONFIGURATION REQUISE

For de plus amples informations, visitez notre page : <http://www.sophos.fr/products/all-sysreqs.html>

### Configuration requise pour Enterprise Console

<b>Plates-formes prises en charge</b>	Windows 95/98/NT4/2000/XP/2003/ Vista/2008/7 Mac OS X Linux UNIX
<b>Matériel</b>	Pentium 2.0 GHz minimum ou équivalent
<b>Serveur d'administration</b>	Windows Server 2008 Windows Server 2003 et R2 Windows 2000 Server VMWare ESX VMWare Workstation VMWare Server
<b>Serveur d'administration Sophos NAC</b>	Windows Server 2008 32 bits Windows Server 2003 et R2 32 bits
<b>Console à distance</b>	Windows Server 2008 Windows Server 2003 et R2 Vista Windows XP Professional Windows 2000 Professional ou Server VMWare ESX VMWare Workstation VMWare Server
<b>Espace disque</b>	Minimum 150 Mo MSDE 2 Go SQL 2005 aucune limite SQL 2008 aucune limite SQL 2005 Express Edition 4 Go SQL 2008 Express Edition 4 Go SQL Server 2000 2 Go
<b>Mémoire</b>	1 Go minimum pour l'exécution de Sophos NAC Manager

### Configuration requise pour l'agent de conformité de Sophos NAC

<b>Plates-formes prises en charge</b>	Windows 2000/XP/Vista
<b>Espace disque</b>	20 Mo minimum
<b>Mémoire</b>	512 Mo de mémoire vive recommandés

### Configuration requise pour Sophos SafeGuard Disk Encryption

<b>Mémoire</b>	Windows 7/Vista : 1 Go recommandé Windows XP : 512 Mo recommandé
----------------	---

### Sophos Endpoint Security and Control pour Windows

Plates-formes prises en charge	
Windows 95/98/NT4/2000 and 2000 Pro/XP Home and Pro/2003/Vista/2008/7	
Windows Netbooks	
Windows XPe	
Windows Embedded Standard	
WePOS	
VMWare ESX	
VMWare Workstation	
VMWare Server	
Espace disque	
Windows 2000/XP/2003/Vista/2008/7	120 Mo minimum
Windows Me/98/95/NT4	90 Mo minimum
Mémoire	
Windows 2000/XP/2003/Vista/2008/7	256 Mo recommandés
Windows Me/98/95	64 Mo recommandé
Windows NT4	256 Mo recommandé

### Configuration requise pour Sophos Client Firewall

<b>Plates-formes prises en charge</b>	2000 Pro/XP Home et Pro/Vista
<b>Espace disque</b>	100 Mo d'espace libre minimum
<b>Mémoire</b>	320 Mo de RAM recommandé
<b>Processeur</b>	Type Pentium 300 MHz

### Réseau de test de Sophos Anti-Virus pour Mac OS X

Vous aurez besoin de paramétrer un réseau de test d'ordinateurs exécutant Mac OS X. Vous aurez aussi besoin d'attribuer à un ordinateur la fonction de serveur contenant le répertoire d'installation centralisée (CID), le dossier utilisé pour télécharger Sophos Anti-Virus et le déployer sur le reste du réseau. Le répertoire d'installation centralisée doit également accueillir Sophos Update Manager, qui permet la mise à jour des ordinateurs Mac OS X, l'installation des fichiers d'identités virales les plus récents et l'application des paramètres de configuration.

### Configuration requise pour Sophos Anti-Virus pour Mac OS X

<b>Plates-formes prises en charge</b>	Mac OS X 10.2 ou supérieur :
<b>Espace disque</b>	90 Mo minimum
<b>Mémoire</b>	128 Mo de RAM recommandé
<b>Processeur</b>	Macs Intel et PowerPC

## ANNEXE II

## LE “VIRUS” TEST EICAR

### A PROPOS DU FICHIER TEST EICAR

Le fichier test antivirus standard EICAR\* peut être utilisé sans danger lors de tests car il ne s'agit pas d'un virus et il n'inclut pas de fragments de code viral. Il s'agit d'un programme DOS légitime constitué entièrement de caractères ASCII imprimables. Le fichier permet de simuler en toute sécurité ce qui se produit lorsque Sophos Anti-Virus détecte du code malveillant. Lorsque vous tentez d'exécuter le fichier, il est détecté comme s'il s'agissait d'un véritable virus et des messages d'alerte personnalisables sont générés.

Le fichier EICAR permet également de découvrir les différents types de rapports pouvant être générés.

Le fichier test peut être téléchargé sur le site [www.eicar.org](http://www.eicar.org)

### Remarque

Le fichier EICAR n'étant pas un vrai virus, il ne peut pas être nettoyé par Sophos Anti-Virus et doit donc être supprimé manuellement.

## ANNEXE III

## AUTRES PRODUITS ET SERVICES SOPHOS

### Sophos Security and Data Protection

#### *Sophos Email Security and Data Protection*

Sophos Email Security and Control offre un choix de solutions logicielles et d'appliances de messagerie pleinement intégrées qui assurent une protection efficace et intelligente contre les virus, spywares, chevaux de Troie, spam et le contenu offensant.

#### *Sophos Web Security and Control*

Sophos Web Security and Control contient les logiciels nécessaires et une appliance web pleinement intégrée offrant une protection contre toute la gamme des menaces Internet. Une infrastructure complète de navigation sécurisée permet une administration simple de la sécurité sur Internet.

#### *Sophos NAC Advanced*

Sophos NAC Advanced est une suite logicielle qui vous permet de bénéficier d'un contrôle absolu sur tout ce qui se connecte à votre réseau. Sophos NAC Advanced s'adresse aux entreprises qui nécessitent un contrôle des politiques plus avancé que celui offert par Endpoint Security and Data Protection.

#### *Sophos SafeGuard Enterprise*

SafeGuard Enterprise est une plate-forme modulaire de contrôle et de protection des informations qui applique aux PC et aux médias amovibles une politique de sécurité dans des environnements hétérogènes. Il s'agit d'un produit totalement transparent pour les utilisateurs finaux, qui s'administre facilement depuis une console centrale unique. SafeGuard Enterprise offre une sécurité multiniveau des données des systèmes d'extrémité en associant le chiffrement et la prévention des fuites de données (DLP).

#### *SAV Interface*

SAV Interface™ permet aux éditeurs de sécurité, aux OEM, aux FAI et aux FAH d'intégrer la détection des malwares Sophos dans leurs propres pare-feu, passerelles et autres solutions semblables normalisés.

#### *Solutions PME Sophos*

Les solutions PME Sophos permettent aux entreprises ayant des ressources informatiques limitées de bénéficier d'une protection antivirus, antispyware et antispam considérée comme l'une des meilleures du marché.

## Sophos Alert Services

Le **service Sophos ZombieAlert™** vous avertit immédiatement lorsque des spammeurs ont piraté les ordinateurs de votre entreprise pour envoyer du spam ou lancer des attaques par déni de service.

[www.sophos.com/products/enterprise/alert-services/zombiealert.html](http://www.sophos.com/products/enterprise/alert-services/zombiealert.html)

Le **service Sophos PhishAlert™** transmet des alertes rapides pratiquement en temps réel sur les campagnes de phishing, de manière à ce que vous puissiez prendre des mesures pour fermer le site web d'imitation et protéger les clients de votre entreprise.

[www.sophos.com/products/enterprise/alert-services/phishalert.html](http://www.sophos.com/products/enterprise/alert-services/phishalert.html)

Le **service Sophos WebAlert™** envoie un avertissement si des pages de votre site Internet ont été piratées ou hébergent du malware.

[www.sophos.com/products/enterprise/alert-services/webalert.html](http://www.sophos.com/products/enterprise/alert-services/webalert.html)

## Sophos Global Support Services

Le support ne consiste pas seulement à vous assister lors de l'installation du produit ou à vous proposer des mises à jour. Notre objectif premier est de partager avec vous tout notre savoir-faire afin de vous offrir la meilleure protection possible.

Notre équipe d'experts est formée aux solutions Sophos ainsi qu'aux technologies de fabricants tiers.

A chaque fois que vous contactez les Services du support international de Sophos, vous pouvez être sûr que vous allez entrer en communication avec un employé de Sophos entièrement formé à nos produits et pas avec un centre d'appels délocalisé à l'étranger.

## Le Support Technique

Une équipe international d'experts Sophos assure toute l'année une assistance 24h/24 pour l'installation, la configuration et la mise à niveau de nos produits et pour la résolution de tout problème technique.

Le support Standard, disponible 24 heures sur 24, 7 jours sur 7, est inclus sans frais supplémentaire avec chaque licence. Pour les licences perpétuelles, le support Standard doit être acheté séparément. Les supports Premium et Platinum sont proposés moyennant un supplément calculé sur le coût de votre licence et incluent des contrats de services par lesquels nous nous engageons à verser une compensation financière au client si nous ne respectons pas les temps de réponse définis par le contrat.

## Services professionnels

Les services professionnels de Sophos vous offrent toutes les compétences nécessaires pour installer et maintenir à jour vos solutions de sécurité. Nous disposons d'un large éventail de services standards et personnalisés pour vous aider en cas de besoin. Ces services peuvent être assurés dans vos locaux ou à distance et assurent à votre entreprise un retour sur investissement optimal dans les produits Sophos.

## Formation Technique

Le service de formation technique Sophos propose dans le monde entier des formations et des ateliers pour assister les entreprises dans le traitement des menaces de plus en plus complexes et à caractère évolutif. Avec des formations incluant la sécurité des systèmes d'extrémité, des messagerie et sur le web, nos packages personnalisés peuvent répondre à vos besoins spécifiques.

Pour plus d'informations, visitez [www.sophos.fr/support](http://www.sophos.fr/support)

## Outils gratuits

Sophos propose un certain nombre d'outils pouvant être utilisés pour combattre les vulnérabilités et les menaces. Disponibles sous forme de fichiers téléchargeables, ils utilisent nos technologies et nos données les plus récentes.

### *Sophos Computer Security Scan*

<http://www.sophos.fr/products/free-tools/sophos-computer-security-scan.html>

Utilisez notre Sophos Computer Security Scan pour identifier toutes les menaces non détectées par votre logiciel actuel. Détectez les malwares ainsi que les périphériques et applications indésirables tels que les supports amovibles, les logiciels peer-to-peer, les jeux, etc. pouvant causer une perte de données

### *Test d'évaluation des systèmes d'extrémité*

[www.sophos.fr/products/free-tools/sophos-endpoint-assessment-test/](http://www.sophos.fr/products/free-tools/sophos-endpoint-assessment-test/)

Utilisez notre Test d'évaluation des systèmes d'extrémité pour détecter tous les risques de sécurité de vos ordinateurs. Vérifiez s'il manque des correctifs OS et si toutes les applications de sécurité sont à jour et activées.

### *Outil de recherche d'applications*

[www.sophos.fr/products/enterprise/applicationdiscovery/eval](http://www.sophos.fr/products/enterprise/applicationdiscovery/eval)

Utilisez notre outil gratuit de recherche d'applications pour identifier et localiser sur votre réseau des applications non autorisées que Sophos Anti-Virus peut contrôler. L'outil fonctionne avec votre logiciel antivirus existant.

### *Test de détection des menaces de Sophos*

[www.sophos.fr/products/free-tools/sophos-threat-detection-test.html](http://www.sophos.fr/products/free-tools/sophos-threat-detection-test.html)

Utilisez notre Test de détection des menaces pour vérifier votre protection antivirus existante. Cet outil permet d'effectuer un contrôle rapide et de rechercher tous les virus, spywares, adwares ou menaces du jour zéro que votre protection antivirus actuelle a pu omettre. Le test peut être effectué sans désinstaller ou désactiver votre logiciel antivirus actuel.

### *Sophos Anti-Rootkit*

[www.sophos.fr/products/free-tools/sophos-anti-rootkit.html](http://www.sophos.fr/products/free-tools/sophos-anti-rootkit.html)

Utilisez notre logiciel gratuit Sophos Anti-Rootkit pour éliminer les rootkits. Cet outil contrôle, détecte et supprime tout rootkit caché sur votre ordinateur, grâce à sa technologie de détection avancée.

Pour plus d'informations sur les outils gratuits Sophos, visitez notre page : <http://www.sophos.fr/products/free-tools/>

