

Sophos Endpoint Security and Control 9.7

Guide de configuration des stratégies

Date du document : avril 2011



Table des matières

1	À propos de ce guide.....	3
2	Recommandations d'utilisation générale des stratégies.....	4
3	Paramétrage d'une stratégie de mise à jour.....	5
4	Paramétrage des stratégies antivirus et HIPS.....	7
5	Paramétrage des stratégies de pare-feu.....	10
6	Configuration des stratégies du contrôle des applications.....	14
7	Paramétrage des stratégies de contrôle des périphériques.....	16
8	Paramétrage des stratégies de contrôle des données.....	18
9	Paramétrage des stratégies de protection antialtération.....	23
10	Paramétrage des stratégies NAC.....	25
11	Recommandations à suivre pour le contrôle.....	27
12	Utilisation des contrôles sur accès.....	28
13	Utilisation des contrôles planifiés.....	29
14	Utilisation des contrôles à la demande	30
15	Exclusion d'éléments du contrôle.....	31
16	Support technique.....	32
17	Mentions légales.....	33

1 À propos de ce guide

Ce guide vous propose des instructions de configuration des stratégies pour le logiciel Sophos Endpoint Security and Control.

En particulier, il vous aide à :

- Comprendre les recommandations d'utilisation des stratégies.
- Configurer et déployer chaque stratégie par type.
- Utiliser les options de contrôle pour rechercher les éléments.
- Déterminer quels éléments à exclure du contrôle.

Ce guide s'adresse à vous si :

- Vous utilisez l'Enterprise Console.
- Vous voulez des conseils sur les meilleures options à utiliser pour la configuration et le déploiement des stratégies.

Consultez le *Guide de démarrage rapide de Sophos Endpoint Security and Control* avant de lire ce guide.

Tous les documents concernant l'Enterprise Console sont disponibles sur www.sophos.fr/support/docs/Enterprise_Console-all.html.

2 Recommandations d'utilisation générale des stratégies

Lorsque vous installez l'Enterprise Console, les stratégies par défaut sont créées pour vous. Ces stratégies s'appliquent à tous les groupes que vous créez. Les stratégies par défaut sont conçues pour garantir un niveau efficace de protection. Si vous souhaitez utiliser les fonctions de contrôle des applications, de contrôle des périphériques, de contrôle des données, de protection antialtération ou de contrôle d'accès réseau, créez de nouvelles stratégies ou modifiez les stratégies par défaut. Lors du paramétrage des stratégies, envisagez les actions suivantes :

- Utilisez les paramètres par défaut de la stratégie lorsque possible.
- Prenez en compte le rôle de l'ordinateur lors du changement des paramètres de la stratégie par défaut ou lors de la création de nouvelles stratégies (par exemple, un ordinateur de bureau ou un serveur).
- Utilisez l'Enterprise Console pour tous les paramètres de stratégie centralisés et définissez les options dans l'Enterprise Console plutôt que sur l'ordinateur lui-même lorsque c'est possible.
- Définissez les options sur l'ordinateur lui-même uniquement lorsque vous avez besoin d'une configuration temporaire pour cet ordinateur ou pour les éléments pour lesquels la configuration centralisée est impossible comme par exemple les options de contrôle avancées.
- Créez un groupe et une stratégie séparés pour les ordinateurs nécessitant une configuration spéciale à longue échéance.

3 Paramétrage d'une stratégie de mise à jour

La stratégie de mise à jour spécifie les ordinateurs qui reçoivent les nouvelles définitions de menaces et les mises à jour des logiciels Sophos. Un abonnement logiciel permet de spécifier quelles versions des logiciels pour systèmes d'extrémité sont téléchargées depuis Sophos pour chaque plate-forme. La stratégie de mise à jour par défaut vous permet d'installer et de mettre à jour les logiciels spécifiés dans l'abonnement "Recommended". Lors du paramétrage de votre stratégie de mise à jour, envisagez les actions suivantes :

- Abonnez-vous aux versions "Recommandées" de votre logiciel afin d'être sûr qu'il sera maintenu à jour automatiquement. Toutefois, si vous voulez évaluer les nouvelles versions des logiciels avant de les placer sur votre réseau principal, vous pouvez utiliser des versions fixes des logiciels sur le même réseau tout en évaluant les nouvelles versions. Tous les mois, les versions fixes sont mises à jour avec des nouvelles données de détection des menaces, mais pas avec la dernière version du logiciel.
- Assurez-vous que le nombre de groupes utilisant la même stratégie de mise à jour est gérable. Vous ne devez pas avoir plus de 1000 ordinateurs se mettant à jour depuis le même emplacement. Le nombre idéal pour une mise à jour optimale depuis le même emplacement est de 600-700 ordinateurs.

Remarque : le nombre d'ordinateurs pouvant se mettre à jour depuis le même répertoire dépend du serveur contenant ce répertoire et de la connectivité du réseau.

- Par défaut, les ordinateurs se mettent à jour depuis un emplacement principal unique. Nous recommandons toutefois de toujours paramétrer un emplacement secondaire pour les mises à jour. Si les ordinateurs d'extrémité ne sont pas en mesure de contacter leur emplacement principal, ils tentent de se mettre à jour depuis leur emplacement secondaire. Pour plus d'informations, reportez-vous à l'Aide de la Sophos Enterprise Console.
- Pour les utilisateurs de portables dont l'itinérance est forte au niveau national ou international au sein d'une entreprise, autorisez l'itinérance dans une stratégie de mise à jour. Lorsque cette option est activée, les portables itinérants tentent de localiser l'emplacement le plus proche et de se mettre à jour depuis celui-ci en interrogeant les ordinateurs fixes sur le même réseau local auxquels ils sont connectés, réduisant ainsi les retards de mise à jour et les coûts de bande passante. S'il reçoit plusieurs emplacements, l'ordinateur portable détermine lequel est le plus proche et l'utilise. Si aucun emplacement ne fonctionne, l'ordinateur portable utilise l'emplacement principal (puis l'emplacement secondaire) défini dans sa stratégie de mise à jour. L'itinérance est uniquement prise en charge si vous utilisez Sophos Update Manager et ne fonctionne que si le poste d'extrémité itinérant est mis à jour depuis un emplacement géré par la même instance de l'Enterprise Console que celle qui administre le poste d'extrémité. Pour plus d'informations, reportez-vous à l'Aide de la Sophos Enterprise Console.
- En cas de doutes concernant les performances sur des ordinateurs à faibles spécifications, abonnez-vous à une version fixe des logiciels et changez manuellement l'abonnement logiciels lorsque vous êtes prêt à mettre à jour les logiciels sur ces ordinateurs. Cette option garantit la mise à jour de ces ordinateurs avec des nouvelles données de détection des menaces. Autrement, vous pouvez exécuter les mises à jour moins souvent (deux ou trois fois par jour) sur les ordinateurs à faibles spécifications ou à des heures précises en dehors des heures habituelles (en soirée ou le week-end).



Avertissement : la réduction des mises à jour augmente les risques de menaces pour votre sécurité.

4 Paramétrage des stratégies antivirus et HIPS

4.1 Paramètres recommandés

La stratégie antivirus et HIPS définit la manière dont le logiciel de sécurité effectue le contrôle des ordinateurs à la recherche de virus, chevaux de Troie, vers, spywares, adwares, applications potentiellement indésirables (PUA), comportements et fichiers suspects et la manière dont il les nettoie. Lorsque vous paramétrez votre stratégie antivirus et HIPS, envisagez les actions suivantes :

- La stratégie antivirus et HIPS par défaut assure la protection des ordinateurs contre les virus et autres malwares. Toutefois, vous pouvez créer de nouvelles stratégies ou changer la stratégie par défaut pour activer la détection d'autres applications ou comportements indésirables.
- Activez la protection Live Sophos qui, grâce à son service de recherche en ligne, décide instantanément si un fichier suspect est une menace et qui effectue la mise à jour en temps réel de votre logiciel Sophos. L'option **Activer la protection Live** est uniquement activée par défaut pour les nouvelles installations du logiciel. Pour les mises à niveau du logiciel, vous devez activer cette option. Pour profiter pleinement de la protection Live Sophos, nous vous recommandons également de sélectionner l'option **Envoyer automatiquement les échantillons de fichiers à Sophos**.
- Utilisez l'option **Alerter uniquement** pour détecter uniquement les comportements suspects. En définissant tout d'abord une stratégie qui édite uniquement des rapports, vous avez une meilleure visibilité des comportements suspects sur votre réseau. Cette option est activée par défaut et doit être dessélectionnée dès que le déploiement de la stratégie est terminé afin de bloquer les programmes et les fichiers.

4.2 Comment déployer la stratégie antivirus et HIPS

Nous vous recommandons de déployer la stratégie antivirus et HIPS comme suit :

1. Créez des stratégies différentes pour des groupes différents.
2. Déterminez les exclusions du contrôle sur accès pour les répertoires ou les ordinateurs avec des bases de données volumineuses ou des fichiers qui changent fréquemment. Assurez-vous par ailleurs que les contrôles planifiés sont exécutés. Vous pouvez, par exemple, exclure des répertoires particuliers sur les serveurs Exchange ou sur d'autres serveurs sur lesquels les performances peuvent être affectées. Pour plus d'informations, consultez l'article 12421 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/12421.html>).
3. Définissez les options de la protection Live Sophos. Cette fonction offre la protection la plus récente contre les menaces grâce à son service de recherche en ligne qui décide

instantanément si un fichier suspect est une menace et grâce à la mise à jour en temps réel de votre logiciel Sophos. Les options suivantes sont disponibles :

- **Activer la protection Live** : si le contrôle antivirus identifie un fichier comme étant suspect sur l'ordinateur mais ne peut pas déterminer s'il s'agit d'un fichier sain ou malveillant en se basant sur les fichiers d'identité des menaces (IDE) présents sur l'ordinateur, certaines caractéristiques du fichier (sa somme de contrôle et d'autres attributs) sont envoyés à Sophos pour une analyse approfondie. Le service de recherche en ligne de Sophos effectue une recherche instantanée d'un fichier suspect dans la base de données des SophosLabs. Si le fichier est identifié comme sain ou malveillant, la décision est renvoyée à l'ordinateur et l'état du fichier est automatiquement mis à jour.

Cette option est uniquement activée par défaut pour les nouvelles installations du logiciel. Pour les mises à niveau du logiciel, vous devez activer cette option.

- **Envoyer automatiquement les échantillons de fichiers à Sophos** : si un fichier est jugé potentiellement malveillant mais ne peut pas être identifié avec certitude comme malveillant d'après ses seules caractéristiques, la protection Live Sophos permet à Sophos de demander un échantillon du fichier. Si l'option Envoyer automatiquement les échantillons de fichiers à Sophos est activée et si Sophos ne détient encore pas d'échantillon du fichier, ce dernier sera soumis automatiquement. La soumission de tels échantillons de fichiers aide Sophos à améliorer en permanence la détection des malwares sans aucun risque de faux positifs.

Important : vous devez vous assurer que le domaine Sophos auquel les données des fichiers sont envoyées est fiable dans votre solution de filtrage web. Pour plus de détails, consultez l'article 62637 de la base de connaissances du support technique de Sophos (<http://www.sophos.fr/support/knowledgebase/article/62637.html>). Si vous utilisez une solution Sophos de filtrage web, par exemple l'appliance web WS1000, aucune opération de votre part n'est nécessaire. Les domaines sont déjà fiables.

4. Détectez les virus et les spywares.
 - a) Assurez-vous que le contrôle sur accès est activé ou planifiez un contrôle intégral du système pour détecter les virus et les spywares. Le contrôle sur accès est activé par défaut. Pour plus d'informations, reportez-vous aux sections [Utilisation des contrôles sur accès](#) à la page 28 ou [Utilisation des contrôles planifiés](#) à la page 29.
 - b) Sélectionnez les options de nettoyage pour les virus/spywares.
5. Détectez les fichiers suspects.

Les fichiers suspects contiennent certaines caractéristiques communes à celles des programmes malveillants mais pas suffisamment pour que le fichier soit identifié en tant que nouvelle pièce de programmes malveillants.

 - a) Activez le contrôle sur accès ou planifiez un contrôle intégral du système pour détecter les fichiers suspects.
 - b) Sélectionnez l'option **Fichiers suspects (HIPS)**.
 - c) Sélectionnez les options de nettoyage pour les fichiers suspects.
 - d) Autorisez de manière appropriée tous les fichiers dont l'exécution est permise.
6. Détectez les comportements suspects et les dépassements de la mémoire tampon.

Les détections des comportements suspects et des dépassements de la mémoire tampon surveillent continuellement les processus en cours pour déterminer si un programme affiche un comportement suspect. Ces détections sont utiles pour bloquer les défauts de sécurité.

- a) Utilisez l'option **Alerter uniquement** pour ne détecter que les comportements suspects et les dépassements de la mémoire tampon. Cette option est activée par défaut.
- b) Autorisez tous les programmes ou fichiers que vous souhaitez continuer à exécuter à l'avenir.
- c) Configurez votre stratégie pour bloquer les programmes et fichiers qui sont détectés en dessélectionnant l'option **Alerter uniquement**.

Cette approche évite le blocage des programmes et des fichiers dont vos utilisateurs pourraient avoir besoin. Pour plus d'informations, consultez l'article 50160 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/50160.html>).

7. Déterminez les adwares et les PUA.

Lorsque vous lancez un contrôle à la recherche d'adwares et de PUA pour la première fois, le contrôle peut générer un grand nombre d'alertes pour les applications qui sont déjà en cours d'exécution sur votre réseau. En commençant par exécuter un contrôle planifié, vous traitez de manière plus sûre les applications qui sont déjà en cours d'exécution sur votre réseau.

- a) Planifiez un contrôle intégral du système pour détecter tous les adwares et PUA.
- b) Autorisez ou désinstallez toutes les applications détectées par le contrôle.
- c) Sélectionnez l'option de contrôle sur accès **Adwares et PUA** pour détecter les adwares et les PUA à venir.

Pour plus d'informations, consultez l'article 13815 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/13815.html>).

8. Déterminez les menaces dans les pages Web.

- a) Assurez-vous que l'option **Bloquer l'accès aux sites Web malveillants** est définie sur **Activé** pour garantir le blocage des sites Web malveillants. Cette option est activée par défaut.
- b) Paramétrez l'option **Contrôle des téléchargements** sur **Activé** ou sur **Identique à celui sur accès** pour contrôler et bloquer toutes données malveillantes téléchargées. L'option **Identique à celui sur accès**, paramètre par défaut, active le contrôle des téléchargements seulement lorsque le contrôle sur accès est activé.
- c) Selon le cas, autorisez tous les sites Web qui sont autorisés.

Pour plus d'informations sur le paramétrage de la stratégie antivirus et HIPS, reportez-vous à l'Aide de la Sophos Enterprise Console.

5 Paramétrage des stratégies de pare-feu

5.1 Paramètres recommandés

La stratégie de pare-feu définit la manière dont le pare-feu assure la protection des ordinateurs. Lors du paramétrage de votre stratégie de pare-feu, envisagez les actions suivantes :

- Lorsque Sophos Client Firewall est installé, le paramètre du pare-feu Windows est désactivé, par conséquent, si vous utilisez le pare-feu Windows, notez vos configurations existantes et déplacez-les dans Sophos Client Firewall.
- Utilisez le mode **Autoriser par défaut** pour détecter le trafic, les applications et les processus, mais sans les bloquer. Si vous définissez d'abord une stratégie qui édite uniquement des rapports, ceci vous permettra d'avoir une meilleure visibilité de l'activité du réseau.
- Utilisez l'Observateur d'événements du pare-feu pour voir le trafic, les applications et les processus utilisés. L'Observateur d'événements vous facilite également la tâche de création de règles d'autorisation ou de blocage du trafic, des applications et des processus signalés. Vous accédez à l'Observateur d'événements en cliquant sur **Affichage > Événements du pare-feu**.
- Utilisez le mode **Interactif** sur des ordinateurs de test pour voir les boîtes de dialogue d'apprentissage, configurer et identifier les applications que vous utilisez et importer et modifier les règles établies par ce processus.
- En mode **Interactif**, nous vous recommandons de dessélectionner l'option **Afficher une alerte sur la console d'administration en cas de modifications locales de règles globales, d'applications, de processus ou de sommes de contrôle** afin d'éviter des alertes "Diffère de la stratégie" lorsque les utilisateurs répondent aux boîtes de dialogue d'apprentissage.
- Autorisez l'utilisation d'un navigateur Web, de la messagerie électronique et du partage de fichiers et d'imprimantes.
- Nous vous recommandons de ne pas changer les paramètres ICMP par défaut, les règles globales et les règles d'applications sauf si vous êtes un utilisateur confirmé en administration réseau.
- Nous vous conseillons dans la mesure du possible de créer des règles d'applications plutôt que des règles globales.

5.2 Configuration du pare-feu en emplacement double

L'option d'emplacement unique s'adresse aux ordinateurs qui sont connectés en permanence à un réseau unique comme les postes de travail. L'option d'emplacement double est disponible si vous voulez que le pare-feu utilise des paramètres différents en fonction de l'emplacement où les ordinateurs sont utilisés, par exemple, au bureau et en dehors du bureau. Il peut être judicieux de paramétrer un emplacement double pour les ordinateurs portables.

Si vous sélectionnez l'emplacement double, nous vous recommandons de paramétrer vos options de configuration d'emplacement principal et secondaire comme suit :

- Paramétrez votre emplacement principal en tant que réseau que vous contrôlez (par exemple, le réseau professionnel) et votre emplacement secondaire en tant qu'emplacement étant hors de votre contrôle.
- Paramétrez votre emplacement principal de manière à ce qu'il ait un accès plus facile et votre emplacement secondaire de manière à ce qu'il ait un accès plus restreint.
- Lors de la configuration de vos options de détection de l'emplacement principal, nous recommandons généralement d'utiliser la détection DNS sur des réseaux étendus et complexes et d'utiliser la détection passerelle pour les réseaux de petite taille et simples. La détection DNS nécessite l'utilisation d'un serveur DNS mais elle est généralement plus facile à gérer que la détection passerelle. Si le matériel utilisé pour la détection passerelle tombe en panne, la reconfiguration des adresses MAC est nécessaire et il est possible que les ordinateurs reçoivent par erreur la configuration de l'emplacement secondaire tant que les problèmes de configuration matérielle ne sont pas résolus.
- Si vous utilisez la détection DNS, nous vous recommandons d'ajouter une entrée DNS spécifique à votre serveur DNS dont le nom est inhabituel et qui renvoie une adresse IP localhost également appelée adresse de bouclage ou loopback (127.x.x.x). Ces options rendent pratiquement impossible la détection incorrecte de tout autre réseau auquel vous êtes connecté comme étant votre emplacement principal.
- Dans la section "Emplacement appliqué" de la configuration avancée de la stratégie de pare-feu, sélectionnez la configuration du pare-feu que vous souhaitez appliquer à l'ordinateur. Si vous souhaitez que la configuration appliquée dépende de l'emplacement de l'ordinateur, sélectionnez l'option **Appliquer la configuration pour l'emplacement détecté**. Si vous souhaitez appliquer manuellement la configuration principale ou secondaire, sélectionnez l'option appropriée.



Avertissement : il est vivement recommandé d'utiliser avec précaution les règles de sous-réseau local comme configurations secondaires. S'il s'agit d'un ordinateur portable utilisé en dehors du bureau, il peut se connecter à un sous-réseau inconnu. Dans ce cas, il se peut que les règles de pare-feu de la configuration secondaire qui utilisent l'adresse du sous-réseau local autorisent le trafic inconnu.

5.3 Quand faut-il bloquer ou autoriser le trafic, les applications et les processus ?

Nous vous recommandons de bloquer ou d'autoriser le trafic, les applications et les processus comme suit :

- Si le pare-feu est en mode **Interactif**, apprenez à vos utilisateurs quel trafic, quelles applications ou quels processus doivent être bloqués ou autorisés.
- Si le pare-feu est en mode **Bloquer par défaut**, l'utilisateur ne reçoit pas les boîtes de dialogue d'apprentissage et l'administrateur est responsable du blocage ou de l'autorisation de tout le trafic, de toutes les applications ou de tous les processus depuis l'Enterprise Console.

- Les options **Bloquer cette fois-ci seulement** sur un ordinateur doivent uniquement être utilisées si l'utilisateur n'est pas sûr s'il doit bloquer le trafic ou non. Les options sont uniquement disponibles sur l'ordinateur lorsque la stratégie est en mode **Interactif**.
- Dans certains cas, le trafic ne doit **pas** être bloqué. Ceux-ci s'appliquent aux règles de somme de contrôle et d'application liées au navigateur Web, à la messagerie électronique, au partage de fichiers et d'imprimantes et à tout autre programme devant accéder à Internet.
- Dès qu'un ordinateur est configuré avec les applications autorisées, les utilisateurs doivent uniquement être invités à effectuer une action lors de l'installation de nouvelles applications ou de correctifs pour les applications existantes (en mode **Interactif**).

5.4 Comment déployer une stratégie de pare-feu

Par défaut, le pare-feu est activé et bloque tout le trafic réseau non indispensable. Par conséquent, configurez-le pour qu'il autorise le trafic, les applications et les processus que vous souhaitez utiliser et testez-le avant d'installer et d'exécuter le pare-feu sur tous les ordinateurs. Nous vous recommandons d'introduire la stratégie de pare-feu comme suit :

1. Préparez votre stratégie ainsi que ce que vous souhaitez qu'elle fasse avant de créer ou de modifier les règles de pare-feu (globale, application ou autre).
2. Utilisez le mode **Autoriser par défaut** pour détecter le trafic habituel, les applications et les processus, mais sans les bloquer.
3. Utilisez l'Observateur d'événements du pare-feu pour voir le trafic, les applications et les processus utilisés. L'Observateur d'événements vous facilite également la tâche de création de règles d'autorisation ou de blocage du trafic, des applications et des processus signalés. Vous accédez à l'Observateur d'événements en cliquant sur **Affichage > Événements du pare-feu**.
4. Créez des règles globales et d'applications personnalisées si nécessaire.

Remarque : votre alternative aux étapes 1 à 4 est de configurer un ordinateur de test en mode **Interactif**, puis d'importer et de modifier les règles établies par ce processus. Pour plus d'informations, reportez-vous à l'Aide de Sophos Endpoint Security and Control.

5. Procédez à un déploiement par phases de Sophos Client Firewall sur votre réseau. Ainsi, vous évitez d'inonder votre réseau de trafic au cours des premières étapes. Déployez d'abord Sophos Client Firewall sur un petit nombre d'ordinateurs pour vous faciliter la surveillance. Ces ordinateurs doivent être représentatifs des différents rôles remplis sur votre réseau.



Avertissement : ne procédez pas au déploiement sur tout votre réseau tant que la configuration n'a pas été soigneusement vérifiée et testée.

- a) Installez et configurez Sophos Client Firewall sur des ordinateurs test.
 - b) Exécutez tous vos programmes et procédures habituels sur ces ordinateurs.
 - c) Recherchez toutes les failles de la configuration de test (par exemple, un accès trop large attribué à certains utilisateurs).
 - d) En cas de besoins différents, procédez à une sous-division du groupe et créez des configurations supplémentaires si nécessaire.
 - e) Dès que vous avez testé les règles, changez le mode de stratégie sur **Bloquer par défaut**, sinon les ordinateurs demeureront non sécurisés.
6. Dès que vous avez terminé la première étape de votre déploiement, préparez le déploiement de Sophos Client Firewall sur tout votre réseau.
- Il est important d'éviter d'inonder le réseau avec trop de trafic. Ne procédez pas au déploiement en une fois sur tout votre réseau.
- Divisez le reste du réseau en groupes faciles à gérer, comme par exemple, un groupe de 100 ordinateurs à la fois.
 - Procédez au déploiement par étapes sur ces groupes.

Pour plus d'informations sur le paramétrage de la stratégie de pare-feu, reportez-vous à l'Aide de la Sophos Enterprise Console. Pour plus d'informations sur les paramètres par défaut du pare-feu, consultez l'article 14464 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/14464.html>).

Pour plus d'informations sur les nouvelles fonctions du pare-feu dans Enterprise Console 4.0, consultez l'article 54750 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/54750.html>).

6 Configuration des stratégies de contrôle des applications

6.1 Paramètres recommandés

La stratégie de contrôle des applications définit quelles applications sont bloquées et autorisées sur vos ordinateurs. Lors du paramétrage de la stratégie de contrôle des applications, envisagez les actions suivantes :

- Utilisez l'option **Détecter mais autoriser l'exécution** pour détecter les applications contrôlées, mais sans les bloquer. Si vous définissez d'abord une stratégie qui édite uniquement des rapports, ceci vous permettra d'avoir une meilleure visibilité des applications utilisées sur tout votre réseau.
- Utilisez l'Observateur d'événements du contrôle des applications afin de pouvoir vérifier l'utilisation des applications au sein de votre entreprise. Vous pouvez accéder à l'Observateur d'événements en cliquant sur **Affichage > Événements du contrôle des applications**.
- Utilisez le Gestionnaire des rapports pour créer des rapports de tendance sur les événements de contrôle des applications par ordinateur ou par utilisateur.
- Envisagez l'utilisation de l'option "Toutes ajoutées par Sophos à l'avenir" pour bloquer toutes les nouvelles applications d'un type spécifique que Sophos ajoute afin de vous éviter de constamment mettre à jour votre stratégie. Par exemple, si vous bloquez actuellement toutes les applications de messagerie instantanée, envisagez de bloquer toutes les nouvelles applications de messagerie instantanée.

6.2 Comment déployer une stratégie de contrôle des applications

Par défaut, toutes les applications et tous les types d'applications sont autorisés. Nous vous recommandons d'introduire le contrôle des applications comme suit :

1. Déterminez les applications que vous voulez contrôler.
2. Activez le contrôle sur accès et sélectionnez l'option **Détecter mais autoriser l'exécution** pour détecter les applications contrôlées, mais sans les bloquer.
Vous avez, à présent, une stratégie de contrôle des applications pour tout votre réseau.
3. Utilisez l'Observateur d'événements du contrôle des applications pour voir quelles applications sont en cours d'utilisation et pour déterminer les applications ou les types d'application que vous souhaitez bloquer. Vous pouvez accéder à l'Observateur d'événements en cliquant sur **Affichage > Événements du contrôle des applications**.
4. Pour accorder un accès différent aux applications selon les multiples groupes d'ordinateurs, créez des stratégies différentes pour des groupes différents. Par exemple, vous pouvez interdire l'utilisation des applications de voix sur IP sur les ordinateurs de l'entreprise, mais autoriser leur utilisation sur les ordinateurs connectés à distance.
5. Déterminez quelles applications ou types d'applications vous voulez bloquer et déplacez-les dans la liste Bloquées.
6. Configurez votre stratégie pour bloquer les applications contrôlées qui sont détectées en dessélectionnant l'option **Détecter mais autoriser l'exécution**.

En choisissant cette approche, vous évitez de générer des grands nombres d'alertes et de bloquer les applications dont vos utilisateurs peuvent avoir besoin. Pour plus d'informations sur le paramétrage de la stratégie de contrôle des applications, reportez-vous à l'Aide de la Sophos Enterprise Console.

7 Paramétrage des stratégies de contrôle des périphériques

7.1 Paramètres recommandés

La stratégie de contrôle des périphériques spécifie quels périphériques de stockage et de réseau sont autorisés à être utilisés sur les ordinateurs. Lors du paramétrage de la stratégie de contrôle des périphériques, envisagez les actions suivantes :

- Utilisez l'option **Détecter mais ne pas bloquer les périphériques** pour détecter les périphériques contrôlés sans les bloquer. Vous devez tout d'abord paramétrer l'état sur **Bloqué** pour chaque type de périphérique que vous voulez détecter. Le logiciel ne contrôle pas les types de périphériques que vous n'avez pas spécifiés. Si vous définissez d'abord une stratégie qui édite uniquement des rapports, ceci vous permettra d'avoir une meilleure visibilité des périphériques utilisés sur tout votre réseau.
- Utilisez l'Observateur d'événements du contrôle des périphériques pour filtrer plus rapidement les événements bloqués que vous souhaitez consulter. Vous accédez à l'Observateur d'événements en cliquant sur **Affichage > Événements du contrôle des périphériques**.
- Utilisez le Gestionnaire des rapports pour créer des rapports de tendance sur les événements de contrôle des périphériques par ordinateur ou par utilisateur.
- Envisagez un contrôle d'accès plus sévère pour les utilisateurs ayant un accès aux informations sensibles.
- Préparez une liste d'exemptions de périphériques avant de déployer une stratégie qui va bloquer les périphériques. Par exemple, si vous souhaitez autoriser l'utilisation des lecteurs optiques à votre équipe de création artistique.
- La catégorie "Périphériques de stockage amovibles sécurisés" peut être utilisée pour autoriser automatiquement les périphériques de stockage USB chiffrés de différents fabricants que nous prenons en charge. Une liste complète de ces fabricants est disponible sur le site Web de Sophos. Pour une liste des périphériques de stockage amovibles sécurisés pris en charge, consultez l'article 63102 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/63102.html>).
- Utilisez le champ **Commentaire** pour identifier la raison de l'exemption d'un périphérique ou pour savoir qui a demandé cette exemption lors de l'ajout d'exemptions de périphériques à la stratégie de contrôle des périphériques.
- Utilisez les options de messagerie de bureau personnalisées pour offrir plus d'assistance à vos utilisateurs lors de la découverte d'un périphérique contrôlé. Par exemple, vous pouvez fournir un lien vers la stratégie d'utilisation des périphériques de votre entreprise.
- Si vous souhaitez activer un périphérique réseau (par exemple, un adaptateur wifi) lorsque l'ordinateur est physiquement déconnecté du réseau, sélectionnez l'option **Bloquer le pont** lors du paramétrage des niveaux d'accès pour les périphériques réseau.

Remarque : le mode Bloquer le pont réduit de manière significative les risques de pont de réseau entre un réseau professionnel et un réseau non professionnel. Ce mode est disponible

pour les types de périphériques sans fil et modem. Ce mode fonctionne en désactivant les adaptateurs réseau sans fil ou modem lorsqu'un système d'extrémité est connecté à un réseau physique (généralement, via une connexion Ethernet). Une fois l'ordinateur déconnecté du réseau physique, les adaptateurs réseau sans fil ou modem sont réactivés de manière transparente.

- Soyez sûr de vouloir bloquer un périphérique avant de déployer votre stratégie. Assurez-vous de bien connaître tous les cas de figure d'utilisation, surtout ceux liés à la Wifi et aux périphériques réseau.



Avvertissement : toute modification des stratégies s'effectue depuis le serveur de l'Enterprise Console vers l'ordinateur via le réseau, par conséquent, dès que le réseau est bloqué, il ne peut pas être débloqué depuis l'Enterprise Console étant donné que l'ordinateur n'accepte aucune configuration supplémentaire depuis le serveur.

7.2 Comment déployer une stratégie de contrôle des périphériques

Par défaut, le contrôle des périphériques est désactivé et tous les périphériques sont autorisés. Nous vous recommandons d'introduire le contrôle des périphériques comme suit :

1. Déterminez les périphériques que vous voulez contrôler.
2. Activez le contrôle des périphériques et sélectionnez l'option **Détecter mais ne pas bloquer les périphériques** pour détecter les périphériques contrôlés, mais sans les bloquer. Vous devez tout d'abord paramétrer l'état sur **Bloqué** pour chaque type de périphérique que vous voulez détecter. Le logiciel ne contrôle pas les types de périphériques que vous n'avez pas spécifiés.
Vous avez, à présent, une stratégie de contrôle des périphériques pour tout votre réseau.
3. Utilisez l'Observateur d'événements du contrôle des périphériques pour voir quelles périphériques sont en cours d'utilisation et pour déterminer les types de périphériques que vous souhaitez bloquer. Vous accédez à l'Observateur d'événements en cliquant sur **Affichage > Événements du contrôle des périphériques**.
4. Pour accorder un accès différent aux périphériques selon les multiples groupes d'ordinateurs, créez des stratégies différentes pour des groupes différents. Par exemple, il se peut que vous ne souhaitiez pas autoriser l'accès des périphériques de stockage amovibles à vos services des ressources humaines et de finances, mais que vous acceptiez de l'autoriser à votre service informatique et de ventes.
5. Exemptez les instances ou les types de modèle que vous ne souhaitez pas bloquer. Par exemple, vous pouvez exempter une clé USB spécifique (instance) ou tous les modems Vodafone 3G (type de modèle).
6. Déterminez quels périphériques vous voulez bloquer et changez leurs états sur **Bloqués**. Vous pouvez aussi autoriser l'accès en lecture seule à certains périphériques de stockage.
7. Configurez votre stratégie pour bloquer les périphériques contrôlés qui sont détectés en dessélectionnant l'option **Détecter mais ne pas bloquer les périphériques**.

En choisissant cette approche, vous évitez de générer un grand nombre d'alertes et de bloquer les périphériques dont vos utilisateurs pourraient avoir besoin. Pour plus d'informations sur le paramétrage de la stratégie de contrôle des périphériques, reportez-vous à l'Aide de la Sophos Enterprise Console.

8 Paramétrage des stratégies de contrôle des données

8.1 Définition de la stratégie de contrôle des données

La stratégie de contrôle des données vous permet de gérer les risques associés au transfert accidentel de données sensibles depuis les ordinateurs.

Chaque entreprise a sa propre définition des données sensibles. Les exemples les plus usuels sont :

- Les dossiers sur les clients contenant des informations personnellement identifiables.
- Les données financières telles que les numéros de carte de crédit.
- Les documents confidentiels.

Lorsque la stratégie de contrôle des données est activée, Sophos surveille l'activité de l'utilisateur à tous les points habituels de sortie de données :

- Le transfert des fichiers sur des périphériques de stockage (stockage amovible, support à lecture optique ou disque).
- Le chargement de fichiers dans des applications (navigateurs Web de l'entreprise, clients de messagerie et clients de messagerie instantanée).

Une règle de contrôle des données est composée de trois éléments :

- Correspondances : les options incluent le contenu des fichiers, les types de fichiers et les noms de fichiers.
- Points à surveiller : les points de surveillance incluent les types de stockage et les applications.
- Actions à prendre : les actions disponibles incluent "Autoriser le transfert de fichiers et journaliser l'événement" (mode surveillance), "Autoriser le transfert après accord de l'utilisateur et journaliser l'événement" (mode formation) et "Bloquer le transfert et journaliser l'événement" (mode restreint).

Par exemple, les règles de contrôle des données peuvent être définies pour consigner le chargement des feuilles de calcul à l'aide d'Internet Explorer ou pour autoriser le transfert d'adresses client sur un DVD dès que le transfert est confirmé par l'utilisateur.

La définition de données sensibles selon leur contenu peut se révéler complexe. Sophos simplifie cette tâche en mettant à disposition une bibliothèque contenant par défaut des définitions de données sensibles appelées Listes de contrôle du contenu. La bibliothèque englobe un large nombre de formats de données personnelles identifiables et de données financières et elle est maintenue à jour par Sophos. Si nécessaire, vous pouvez aussi définir des Listes de contrôle du contenu personnalisées.

De même qu'avec les stratégies Sophos, la stratégie de contrôle des données continue d'être appliquée aux ordinateurs même lorsqu'ils sont déconnectés du réseau de votre entreprise.

8.2 Paramètres recommandés

Lors du paramétrage de la stratégie de contrôle des données, envisagez les actions suivantes :

- Utilisez l'option **Autoriser le transfert de fichiers et journaliser l'événement** pour détecter les données contrôlées, mais sans les bloquer. Si vous définissez d'abord une stratégie qui édite uniquement des rapports, ceci vous permettra d'avoir une meilleure visibilité des données utilisées sur tout votre réseau.
- Utilisez l'option **Autoriser le transfert après accord de l'utilisateur et journaliser l'événement** pour alerter les utilisateurs sur les risques de transfert de documents pouvant contenir des données sensibles. Cette approche réduit les risques de perte de données et a un impact limité sur les activités informatiques.
- Utilisez le paramètre "quantité" des règles de contenu pour configurer le volume de données sensibles que vous voulez trouver avant de déclencher une règle. Par exemple, une règle configurée pour rechercher une adresse postale dans un document va générer plus d'événements de contrôle des données qu'une règle recherchant 50 adresses ou plus.

Remarque : Sophos fournit des paramètres de quantité par défaut pour chaque Liste de contrôle du contenu.

- Utilisez l'Observateur d'événements du contrôle des données pour filtrer plus rapidement les événements que vous souhaitez consulter. Tous les événements et actions de contrôle des données sont journalisés de manière centralisée dans l'Enterprise Console. Vous pouvez accéder à l'Observateur d'événements en cliquant sur **Affichage > Événements du contrôle des données**.
- Utilisez le Gestionnaire des rapports pour créer des rapports de tendance sur les événements de contrôle des données par règle, par ordinateur ou par utilisateur.
- Utilisez les options de messagerie de bureau personnalisées pour offrir plus d'assistance à vos utilisateurs lors du déclenchement d'une action. Par exemple, vous pouvez fournir un lien vers la stratégie de sécurité des données de votre société.
- Utilisez le mode de journalisation détaillée pour recueillir des informations supplémentaires sur les règles de contrôle des données. Dès que l'évaluation de ces règles est terminée, désactivez la journalisation détaillée.

Remarque : la journalisation détaillée doit être activée sur chaque ordinateur. Toutes les données générées sont archivées dans le journal local du contrôle des données de l'ordinateur. Lorsque le mode de journalisation détaillée est activé, toutes les chaînes de caractères qui, dans chaque fichier, correspondent aux données spécifiées dans une règle sont journalisées. Les informations supplémentaires du journal peuvent être utilisées pour identifier des phrases ou des chaînes de caractères dans un document qui ont entraîné le déclenchement d'un événement de contrôle des données.

8.3 Comment déployer une stratégie de contrôle des données

Par défaut, le contrôle des données est désactivé et aucune règle n'est spécifiée pour surveiller ou restreindre le transfert des fichiers sur les périphériques de stockage ou dans les applications. Nous vous recommandons d'introduire le contrôle des données comme suit :

1. Sachez comment le contrôle des données fonctionne sur vos ordinateurs :

- **Périphériques de stockage** : le contrôle des données intercepte tous les fichiers copiés sur les périphériques de stockage surveillés à l'aide de l'Explorateur Windows (qui inclut le bureau Windows). En revanche, les enregistrements directs depuis les applications, telles que Microsoft Word, ou les transferts à l'aide de l'invite de commandes ne sont pas interceptés.

Il est possible de forcer tous les transferts sur les périphériques de stockage surveillés à l'aide de l'Explorateur Windows en utilisant soit l'action "Autoriser le transfert après accord de l'utilisateur et journaliser l'événement", soit l'action "Bloquer le transfert et journaliser l'événement". Dans les deux cas, toute tentative d'enregistrement direct à partir d'une application ou de transfert de fichiers à l'aide de l'invite de commandes est bloquée par le contrôle des données. Une alerte de bureau apparaît et demande à l'utilisateur d'utiliser l'Explorateur Windows pour terminer le transfert.

Lorsqu'une stratégie de contrôle des données contient des règles avec l'option "Autoriser le transfert de fichiers et journaliser l'événement", les enregistrements directs depuis des applications et les transferts à l'aide de l'invite de commandes ne sont pas interceptés. Ce comportement permet à l'utilisateur d'utiliser des périphériques de stockage sans aucune restriction. Par contre, les événements de contrôle des données sont toujours seulement journalisés pour les transferts effectués à l'aide de l'Explorateur Windows.

Remarque : cette restriction ne s'applique pas à la surveillance des applications.

- **Applications** : le contrôle des données intercepte les fichiers et les documents téléchargés en amont dans les applications surveillées. Pour garantir que seuls les chargements de fichiers effectués par les utilisateurs sont surveillés, certains emplacements de fichiers système sont exclus de la surveillance par le contrôle des données. Pour plus d'informations sur le contenu ou sur les actions contrôlés ou non contrôlés dans les applications, reportez-vous à la section [Principes du contrôle des données dans les applications](#) à la page 21.

Remarque : si vous surveillez des clients de messagerie, le contrôle des données contrôle toutes les pièces de jointes de fichiers mais pas le contenu de messagerie. La solution Sophos Email Security and Data Protection peut être utilisée si le contrôle du contenu de la messagerie est requis.

2. Prenez en compte les types d'informations que vous souhaitez identifier et pour lesquels vous souhaitez créer des règles. Sophos propose comme exemple une série de règles que vous pouvez utiliser pour mettre au point votre stratégie de contrôle des données.

Important : lors de la création de règles de contenu, prenez en compte que le contrôle du contenu peut être un processus assez long à effectuer. Il est important de tester l'impact d'une règle de contenu avant de la déployer sur un plus grand nombre d'ordinateurs.

Remarque : lors de la création de votre première stratégie, nous vous recommandons de vous concentrer sur la détection d'un grand nombre d'informations personnellement identifiables dans vos documents. Sophos propose des exemples de règles pour vous aider.

3. Activez le contrôle des données et sélectionnez l'action **Autoriser le transfert de fichiers et journaliser l'événement** dans vos règles pour détecter les données contrôlées, mais sans les bloquer.

Important : nous vous recommandons de configurer toutes les règles afin d'utiliser cette action pour le premier déploiement. Ceci vous permettra d'évaluer l'efficacité des règles sans que cela n'affecte la productivité des utilisateurs.

4. Déployez votre stratégie de contrôle des données sur un petit nombre d'ordinateurs afin de faciliter l'analyse des événements de contrôle des données déclenchés par la stratégie.
5. Utilisez l'Observateur d'événements du contrôle des données pour voir les données en cours d'utilisation, pour déceler toutes les failles de la configuration de test (par exemple, si une règle est trop sensible et génère un plus grand nombre d'événements que prévu). Vous pouvez accéder à l'Observateur d'événements en cliquant sur **Affichage > Événements du contrôle des données**.
6. Dès que la stratégie a été testée, procédez à tous les ajustements nécessaires et déployez-la sur un plus grand nombre d'ordinateurs de votre entreprise. A ce stade, vous pouvez décider de :
 - Changer pour certaines règles les actions selon le cas en **Autoriser le transfert après accord de l'utilisateur et journaliser l'événement** ou **Bloquer le transfert et journaliser l'événement**.
 - Créer des stratégies différentes pour des groupes différents. Vous pouvez, par exemple, autoriser le transfert d'informations personnellement identifiables pour les ordinateurs du service des ressources humaines, mais empêcher cette opération pour tous les autres groupes.

Pour plus d'informations sur le paramétrage de la stratégie de contrôle des données reportez-vous à l'Aide de la Sophos Enterprise Console.

8.4 Principes du contrôle des données dans les applications

Veillez trouver ci-dessous une liste du contenu ou des actions qui sont contrôlés ou non contrôlés dans les applications prises en charge.

Pour obtenir une liste complète des limites connues du contrôle des données, consultez l'article 63016 de la base de connaissances du support technique de Sophos (<http://www.sophos.fr/support/knowledgebase/article/63016.html>).

Applications	Actions de contrôle des données
Navigateurs Web	<p>Ce qui est contrôlé :</p> <ul style="list-style-type: none"> ■ Téléchargements de fichiers en amont ■ Pièces jointes de messagerie Web ■ Téléchargements Microsoft SharePoint en amont <p>Ce qui n'est pas contrôlé</p> <ul style="list-style-type: none"> ■ Le contenu des courriers de messagerie Web ■ Entrées de blogs ■ Téléchargements de fichiers <p>Remarque : dans un petit nombre de cas, les fichiers peuvent être contrôlés lorsqu'ils sont téléchargés.</p>
Clients de messagerie	<p>Ce qui est contrôlé</p> <ul style="list-style-type: none"> ■ Pièces jointes aux courriels <p>Ce qui n'est pas contrôlé</p> <ul style="list-style-type: none"> ■ Contenus des courriels ■ Pièces jointes réacheminées ■ Pièces jointes créées à l'aide de l'option de messagerie "Envoyer" dans les applications (par exemple, Explorateur Windows et Microsoft Office) ■ Les pièces jointes utilisant l'option "Envoyer ce fichier par courrier électronique" dans l'Explorateur Windows ■ Pièces jointes copiées d'un courriel dans un autre courriel ■ Pièce jointes enregistrées <p>Remarque : dans un petit nombre de cas, les fichiers peuvent être contrôlés lorsqu'ils sont enregistrés.</p>
Clients de messagerie instantanée	<p>Ce qui est contrôlé</p> <ul style="list-style-type: none"> ■ Transferts de fichiers <p>Remarque : un fichier peut être contrôlé deux fois : une fois lors du téléchargement dans le client de messagerie et une deuxième fois lors de l'accord par le destinataire. Les deux contrôles ont lieu sur l'ordinateur de l'expéditeur.</p> <p>Ce qui n'est pas contrôlé</p> <ul style="list-style-type: none"> ■ Contenu du message instantané ■ Fichiers envoyés

9 Paramétrage des stratégies de protection antialtération

9.1 Paramètres recommandés

La stratégie de protection antialtération vous permet d'empêcher les utilisateurs non autorisés (administrateurs locaux aux connaissances techniques limitées) de reconfigurer, de désactiver ou de désinstaller les logiciels de sécurité Sophos. Les utilisateurs non autorisés sont ceux qui ne connaissent pas le mot de passe de la protection antialtération.

Remarque : la protection antialtération n'est pas conçue pour assurer la protection contre les utilisateurs expérimentés techniquement. Elle n'assure pas la protection contre les programmes malveillants spécifiquement conçus pour corrompre le fonctionnement du système d'exploitation afin d'éviter d'être détecté. Ce type de programmes malveillants sera uniquement détecté en effectuant un contrôle à la recherche de menaces et de comportements suspects. Pour plus d'informations, reportez-vous à la section [Paramétrage des stratégies antivirus et HIPS](#) à la page 7.

Après que vous avez activé la protection antialtération et créé un mot de passe pour celle-ci, l'utilisateur qui ne connaît pas ce mot de passe ne pourra pas reconfigurer les détections du contrôle sur accès ou des comportements suspects dans Sophos Endpoint Security and Control, désactiver la protection antialtération ou désinstaller les composants Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate ou Sophos Remote Management System) ou Sophos SafeGuard Disk Encryption du Panneau de configuration.

Lors du paramétrage de votre stratégie de protection antialtération, envisagez les actions suivantes :

- Utilisez l'Observateur d'événements de la protection antialtération pour vérifier l'utilisation du mot de passe de la protection antialtération et surveiller la fréquence des tentatives d'altération dans votre entreprise. Vous pouvez voir les événements d'authentification réussis de la protection antialtération (utilisateurs autorisés passant outre la protection antialtération) et les échecs de tentative d'altération des logiciels de sécurité Sophos. Vous accédez à l'Observateur d'événements en cliquant sur **Affichage > Événements de protection antialtération**.

9.2 Comment déployer une stratégie de protection antialtération

Par défaut, la protection antialtération est désactivée. Nous vous recommandons d'introduire la protection antialtération comme suit :

1. Activez la protection antialtération et créez un mot de passe sécurisé de protection antialtération.

Le mot de passe autorise seulement les utilisateurs des postes d'extrémité à reconfigurer, désactiver ou désinstaller les logiciels de sécurité Sophos.

Remarque : la protection antialtération n'affecte pas les membres des groupes SophosUser et SophosPowerUser. Lorsque la protection antialtération est activée, ces utilisateurs peuvent tout de même réaliser toutes les tâches qu'ils ont généralement l'autorisation d'exécuter, sans qu'il soit nécessaire de saisir le mot de passe de la protection antialtération.

2. Si vous avez besoin d'activer ou de désactiver la protection antialtération ou de créer des mots de passe différents pour divers groupes, créez des stratégies différentes pour les différents groupes.

Pour plus d'informations sur le paramétrage de la stratégie de protection antialtération, reportez-vous à l'Aide de la Sophos Enterprise Console.

10 Paramétrage des stratégies NAC

10.1 Utilisation des stratégies NAC prédéfinies

La stratégie NAC définit les conditions auxquelles les ordinateurs doivent se conformer avant qu'ils ne puissent accéder au réseau. Par défaut, Sophos NAC autorise tous les ordinateurs à accéder au réseau. Vous devez configurer une stratégie NAC pour contrôler l'accès.

Utilisez les stratégies prédéfinies pour mettre vos systèmes d'extrémité administrés et non administrés en conformité avec vos stratégies de sécurité. Vous pouvez modifier les stratégies prédéfinies dans le NAC Manager pour changer le mode de stratégie, les profils qui sont dans la stratégie ou les modèles d'accès réseau qui sont appliqués à la stratégie.

Les stratégies suivantes sont disponibles :

- **Default** : cette stratégie est utilisée si l'agent de conformité est installé sur un ordinateur et qu'aucune autre stratégie ne lui a été affectée. Par défaut, le mode de stratégie est paramétré sur Report Only. Cette stratégie effectue des actions d'actualisation sur l'ordinateur si le mode de stratégie est paramétré sur Remediate ou Enforce.
- **Managed** : cette stratégie peut être utilisée pour les ordinateurs administrés avec l'Enterprise Console et sur lesquels l'agent de conformité est installé. Par défaut, le mode de stratégie est paramétré sur Report Only. Cette stratégie effectue des actions d'actualisation sur l'ordinateur si le mode de stratégie est paramétré sur Remediate ou Enforce.
- **Unmanaged** : cette stratégie peut être utilisée pour les ordinateurs situés hors de l'entreprise. Cette stratégie n'effectue pas d'actions d'actualisation sur l'ordinateur. L'agent temporaire de conformité utilise la stratégie Unmanaged.

Pour plus d'informations sur la mise à jour des stratégies prédéfinies, reportez-vous à l'Aide du Sophos NAC Manager.

10.2 Comment déployer une stratégie NAC

Au départ, la stratégie NAC "par défaut" est appliquée à tous les ordinateurs. Si vous voulez modifier les paramètres d'une stratégie ou utiliser une stratégie différente, vous pouvez utiliser Sophos NAC Manager pour modifier une stratégie et l'Enterprise Console pour appliquer cette stratégie aux ordinateurs. Nous vous recommandons d'introduire la stratégie NAC comme suit :

1. Dans l'Enterprise Console, créez ou importez des groupes et déployez Sophos Compliance Agent sur les ordinateurs à l'aide de l'Assistant de protection des ordinateurs.
2. Dans le NAC Manager, assurez-vous que les stratégies NAC contiennent les paramètres, profils et modèles d'accès que vous souhaitez utiliser.
3. Utilisez l'Enterprise Console pour appliquer la stratégie NAC administrée à tous les groupes administrés dans l'Enterprise Console.

Les agents vont commencer à évaluer la conformité en mode de stratégie Report Only.

4. Utilisez les rapports du NAC Manager pour déterminer l'état de conformité actuel des utilisateurs.

Les rapports donnent une vue réaliste de la conformité des utilisateurs avec la stratégie NAC.

5. Utilisez le NAC Manager pour mettre à jour la stratégie NAC administrée. Changez le mode de stratégie de Report Only en Remediate.
6. Utilisez les rapports du NAC Manager pour déterminer l'état de conformité actuel des utilisateurs.

Avec le temps, les ordinateurs non conformes et partiellement conformes doivent être corrigés pour améliorer l'état de conformité global.

7. Utilisez le NAC Manager pour mettre à jour la stratégie NAC administrée. Changez le mode de stratégie de Remediate en Enforce.
8. Utilisez les rapports du NAC Manager pour déterminer l'état de conformité actuel des utilisateurs.

Les ordinateurs non conformes doivent être corrigés ou l'accès au réseau sera refusé à leurs utilisateurs.

Pour plus d'informations sur la configuration de NAC, reportez-vous à l'Aide du Sophos NAC Manager.

11 Recommandations à suivre pour le contrôle

Dans les sections qui suivent, les options de contrôle sont définies dans la stratégie antivirus et HIPS sachant que certaines, comme les extensions et les exclusions, s'appliquent également à la stratégie de contrôle des applications. Lors du choix des options de contrôle, envisagez les actions suivantes :

- Utilisez les paramètres par défaut à chaque fois que c'est possible.
- Paramétrez le contrôle de l'ordinateur depuis l'Enterprise Console à chaque fois que cela vous est possible.
- Prenez en compte le rôle de l'ordinateur (par exemple, ordinateur de bureau ou serveur).
- L'option **Contrôler tous les fichiers** n'est généralement pas nécessaire ou pas recommandée. Sélectionnez plutôt l'option **Contrôler uniquement les exécutables et autres fichiers vulnérables** pour rechercher les menaces découvertes par les SophosLabs. Procédez au contrôle de tous les fichiers uniquement après avoir pris conseil auprès du support technique.
- L'option **Contrôler dans les fichiers archive** ralentit le contrôle et n'est généralement pas requise. Lorsque vous tentez d'accéder au contenu d'un fichier archive, ce fichier est contrôlé automatiquement. Par conséquent, nous vous recommandons de ne pas sélectionner cette option sauf si vous utilisez fréquemment des fichiers archive.
- Nous vous recommandons d'effectuer le contrôle de la mémoire système d'un ordinateur à la recherche des menaces. La mémoire système est utilisée par le système d'exploitation. Vous pouvez contrôler la mémoire système de manière périodique en tâche de fond alors que le contrôle sur accès est activé. Vous pouvez aussi inclure le contrôle de la mémoire système dans le cadre d'un contrôle planifié. L'option **Contrôle de la mémoire système** est uniquement activée par défaut pour les nouvelles installations du logiciel et les nouvelles stratégies. Pour les mises à niveau du logiciel, vous devez activer cette option.

12 Utilisation des contrôles sur accès

Lorsque vous utilisez les contrôles sur accès, envisagez les actions suivantes :

- Utilisez les paramètres par défaut à chaque fois que cela est possible.
- Utilisez l'option de contrôle sur accès **En lecture**. Les options de contrôle **En écriture** et **En renommant** ne sont généralement pas requises mais sont mises à disposition si vous souhaitez bénéficier d'une sécurité maximale. Ces options sont utiles en cas d'épidémies virales.
- Le contrôle sur accès ne détecte pas les virus lorsque certains logiciels de chiffrement sont installés. Modifiez les processus de démarrage afin de vous assurer que ces fichiers sont déchiffrés lorsque le contrôle sur accès commence. Pour plus d'informations sur l'utilisation de la stratégie antivirus et HIPS avec un logiciel de chiffrement, consultez l'article 12790 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/12790.html>).
- Lorsque vous ne sélectionnez pas le contrôle sur accès, assurez-vous que les ordinateurs utilisent les contrôles planifiés. Pour plus d'informations, reportez-vous à la section [Utilisation des contrôles planifiés](#) à la page 29.



Avertissement : la désactivation du contrôle sur accès augmente les risques de menaces pour votre sécurité.

13 Utilisation des contrôles planifiés

Lorsque vous utilisez les contrôles planifiés, envisagez les actions suivantes :

- Utilisez les paramètres par défaut à chaque fois que cela est possible.
- Utilisez les contrôles planifiés pour évaluer les menaces ou estimer la prévalence des applications non désirées ou contrôlées.
- Utilisez les contrôles planifiés sur les répertoires serveur sur lesquels les performances seront affectées par l'utilisation du contrôle sur accès. Par exemple, vous pouvez avoir un groupe de serveurs Exchange qui utilise les contrôles planifiés sur des répertoires spécifiques. Pour plus d'informations, consultez l'article 12421 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/12421.html>).
- Lorsque vous ne sélectionnez pas le contrôle sur accès, assurez-vous que les ordinateurs utilisent les contrôles planifiés. Placez ces ordinateurs dans un groupe et définissez un contrôle planifié.
- Les contrôles planifiés peuvent affecter les performances. Par exemple, si vous procédez au contrôle d'un serveur qui lit les bases de données et y écrit dedans en permanence, prenez en compte le moment où ses performances seront le moins affectées.
- Pour les serveurs, prenez en compte les tâches en cours d'exécution. S'il y a une tâche de sauvegarde, n'exécutez pas le contrôle planifié en même temps que la tâche de sauvegarde.
- Procédez au contrôle à des heures définies. Assurez-vous qu'un contrôle planifié est effectué quotidiennement sur chaque ordinateur (par exemple, tous les jours à 21 heures). Les contrôles planifiés doivent être effectués au moins une fois par semaine sur les ordinateurs.
- L'option **Exécuter le contrôle avec une priorité inférieure** permet l'exécution d'un contrôle planifié sous les systèmes d'exploitation Windows Vista et supérieure avec une priorité inférieure afin que l'opération ait des conséquences minimales sur les applications de l'utilisateur. Cette option est conseillée, même si le contrôle prendra plus de temps que sans cette option.

14 Utilisation des contrôles à la demande

Lorsque vous utilisez les contrôles à la demande, envisagez les actions suivantes :

- Utilisez les contrôles à la demande lorsque l'évaluation ou le nettoyage manuel est nécessaire.

15 Exclusion d'éléments du contrôle

Procédez à l'exclusion d'éléments du contrôle de la manière suivante :

- Utilisez les extensions pour exclure des types de fichiers spécifiques du contrôle.
- Utilisez les exclusions pour exclure des éléments spécifiques, tels que les fichiers ou les lecteurs, du contrôle. Vous pouvez créer des exclusions de lecteur (X:), des exclusions de répertoire (X:\Program Files\Exchsrvr\) ou des exclusions de fichier (X:\Program Files\SomeApp\SomeApp.exe).
- Envisagez d'exclure les périphériques multimédia du contrôle sur accès pour les utilisateurs spécifiques qui les utilisent énormément. Les lecteurs multimédia lisent et écrivent sur les fichiers temporaires et chaque fichier est intercepté et contrôlé à chacune de ses utilisations. Ceci a pour effet de ralentir le contrôle.
- Utilisez l'option **Exclure les fichiers distants** lorsque vous ne souhaitez pas contrôler des fichiers distants (sur les ressources du réseau). Nous vous recommandons de contrôler tous les fichiers distants sur accès, toutefois, vous pouvez sélectionner cette option sur les serveurs de fichiers ou lorsque des fichiers volumineux ou constamment modifiés font l'objet d'un accès à distance.



Avertissement : l'exclusion d'éléments du contrôle augmente les risques de menace pour votre sécurité.

16 Support technique

Vous pouvez obtenir du support technique pour les produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur <http://community.sophos.com/> et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur <http://www.sophos.fr/support/>.
- Téléchargez la documentation des produits sur <http://www.sophos.fr/support/docs/>.
- Envoyez un courriel à support@sophos.fr, y compris le ou les numéros de version du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

17 Mentions légales

Copyright © 2011 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la licence conformément à ses termes ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos et Sophos Anti-Virus sont des marques déposées de Sophos Limited. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

Common Public License

Les logiciels Sophos mentionnés dans le présent document incluent ou peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence Common Public License (CPL), qui, entre autres droits, permettent à l'utilisateur d'avoir accès au code source. La licence CPL exige que pour tout logiciel concédé en licence sous les termes de la licence CPL, qui est distribuée sous un format de code objet, le code source soit aussi mis à disposition de ces utilisateurs sous un format de code objet. Pour chacun de ces logiciels couverts par la licence CPL, le code source est disponible sur commande par courrier postal envoyé à Sophos, par courrier électronique envoyé à support@sophos.fr ou par Internet sur <http://www.sophos.fr/support/queries/enterprise.html>. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur <http://opensource.org/licenses/cpl1.0.php>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.