SOPHOS
Security made simple.

Sophos Enterprise Console
Guide de configuration des stratégies

Version du produit : 5.5

Table des matières

1 À propos de ce guide....4
2 Conseils d'utilisation générale des stratégies....5
3 Création d'une stratégie de mise à jour....6
4 Création de stratégies antivirus et HIPS....8
4.1 Paramètres conseillés....8
4.2 Déploiement de la stratégie antivirus et HIPS....8
5 Création de stratégies de pare-feu....11
5.1 À propos de la stratégie de pare-feu....11
5.2 Planification des stratégies de pare-feu....11
5.3 Paramètres conseillés....12
5.4 Configuration du pare-feu en emplacement double....13
5.5 Déploiement d'une stratégie de pare-feu....14
6 Création de stratégies de contrôle d'applications....16
6.1 Paramètres conseillés....16
6.2 Déploiement d'une stratégie de contrôle d'applications....16
7 Création de stratégies de contrôle des données....18
7.1 Définition d'une stratégie de contrôle des données....18
7.2 Paramètres conseillés....19
7.3 Déploiement d'une stratégie de contrôle des données....20
7.4 Principes du contrôle des données dans les applications....21
8 Création de stratégies de contrôle des périphériques....23
8.1 Paramètres conseillés....23
8.2 Déploiement d'une stratégie de contrôle des périphériques....24
9 Création de stratégies de protection antialtération....25
9.1 À propos de la stratégie de protection antialtération....25
9.2 Déploiement d'une stratégie de protection antialtération....25
10 Création de stratégies de correctif....27
10.1 À propos de la stratégie de correctif....27
10.2 Déploiement d'une stratégie de correctif....27
11 Création de stratégies de contrôle du Web....29
11.1 Paramètres conseillés....29
11.2 Déploiement d'une stratégie de contrôle du Web....30
12 Création des stratégies de prévention des Exploits....32
12.1 Paramètres conseillés....32
12.2 Déploiement d'une stratégie de prévention des Exploits....32

13 Conseils à suivre pour le contrôle.....34
14 Utilisation des contrôles sur accès.....35
15 Utilisation des contrôles planifiés.....36
16 Utilisation des contrôles à la demande.....37
17 Exclusion d’éléments du contrôle.....38
18 Support technique.....39
19 Mentions légales.....40

1 À propos de ce guide

Ce guide décrit les instructions de configuration des stratégies pour les logiciels Sophos Enterprise Console et Sophos Endpoint Security and Control.

Remarque : certaines fonctions seront indisponibles si elles ne font pas partie de votre contrat de licence.

En particulier, il vous aide à :

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

Avant de lire ce guide, consultez le *Guide de démarrage rapide de Sophos Enterprise Console*.

Retrouvez toute la documentation de l'Enterprise Console sur http://www.sophos.com/fr-fr/support/documentation/enterprise-console.aspx.

2 Conseils d'utilisation générale des stratégies

Lorsque vous installez l'Enterprise Console, des 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 des fonctionnalités comme le contrôle d'accès réseau, la gestion des correctifs, le contrôle d'applications, le contrôle des données, le contrôle des périphériques ou la protection antialtération, créez de nouvelles stratégies ou modifiez les stratégies par défaut. Lors de la création des stratégies, envisagez les actions suivantes :

- Utilisez les paramètres par défaut de la stratégie lorsque cela est 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 les options de contrôle avancées.
- Créez un groupe et une stratégie séparés pour les ordinateurs nécessitant une configuration spéciale à longue échéance.

3 Création 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 logiciels permet de spécifier quelles versions des logiciels pour terminaux 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 ». Lorsque vous créez votre stratégie de mise à jour, envisagez les actions suivantes :

- Abonnez-vous aux versions « Recommended » 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 généralement pas avoir plus de 1000 ordinateurs procédant à la mise à jour à partir du 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 à partir d'un seul emplacement principal. Toutefois, nous vous conseillons de configurer également un emplacement secondaire de mise à jour. Si les terminaux ne sont pas en mesure de contacter leur source principale, ils tentent de se mettre à jour depuis leur source secondaire si elle a été spécifiée. Retrouvez plus de renseignements dans l'Aide de Sophos Enterprise Console à la section *Mise à jour des ordinateurs > Configuration de la stratégie de mise à jour*.

- Autorisez l'itinérance sur une stratégie de mise à jour pour les utilisateurs d'ordinateurs portables qui effectuent de nombreux déplacements professionnels au sein de votre entreprise. Lorsque l'option est activée, les ordinateurs portables itinérants recherchent et se mettent à jour à partir de l'emplacement des serveurs de mise à jour le plus proche en envoyant des requêtes aux terminaux fixes se trouvant sur le même réseau local auxquels ils sont connectés, réduisant ainsi les délais de mise à jour et les coûts de bande passante. S'il reçoit plusieurs emplacements, l'ordinateur portable détermine celui qui 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 fonctionnera uniquement si les ordinateurs portables itinérants et les terminaux fixes sont administrés par la même instance de l'Enterprise Console et utilisent le même abonnement logiciels. Tous les pare-feu tiers doivent être configurés afin de permettre les demandes et les réponses de mise à jour des emplacements. Le port 51235 est utilisé par défaut mais il est possible de le changer.

  Retrouvez plus de renseignements dans l'Aide de Sophos Enterprise Console à la section *Mise à jour des ordinateurs > Configuration de la stratégie de mise à jour > Configuration des emplacements du serveur de mise à jour*. Retrouvez une foire aux questions sur l'itinérance dans l'article 112830 de la base de connaissances du support technique Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/112830.aspx).

- 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).

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

4 Création de stratégies antivirus et HIPS

4.1 Paramètres conseillés

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 créez 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.
- Pour bénéficier de tous les avantages de Sophos Live Protection, qui est activée par défaut, nous vous conseillons également de sélectionner l'option **Envoyer automatiquement les échantillons de fichiers à Sophos**.
- Activez la détection du trafic malveillant pour détecter les communications entre les ordinateurs et les serveurs de commande et de contrôle impliqués dans les attaques par botnet ou par autre programme malveillant. L'option **Détecter le trafic malveillant** est activée par défaut sur les nouvelles installations de l'Enterprise Console à partir de la version 5.3. Si vous avez procédé à la mise à niveau vers une version antérieure de l'Enterprise Console, vous allez devoir activer cette option afin de bénéficier de cette fonction.

  Remarque : la détection du trafic malveillant est pour le moment uniquement prise en charge sur les systèmes d'exploitation non serveurs Windows 7 et versions supérieures. Sophos Live Protection doit être activée pour pouvoir utiliser cette fonction.

- Utilisez l'option **Alerter uniquement** pour détecter uniquement les comportements suspects. Si vous définissez d'abord une stratégie qui édite uniquement des rapports, ceci vous permettra d'avoir 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.

Retrouvez plus de renseignements dans l'article 114345 de la base de connaissances du support de Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/114345.aspx).

4.2 Déploiement de la stratégie antivirus et HIPS

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

1. Créer des stratégies différentes pour des groupes différents.
2. Définir les options de Sophos Live Protection. 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. Sophos Live Protection doit être activé pour pouvoir utiliser les fonctions de détection du trafic malveillant et de réputation des téléchargements.

- Assurez-vous d'avoir sélectionné les options **Activer Sophos Live Protection pour le contrôle sur accès** et **Activer Sophos Live Protection pour le contrôle à la demande**. Si le contrôle antivirus identifie un fichier suspect sur l'ordinateur mais ne peut pas déterminer s'il s'agit d'un fichier sain ou malveillant à partir des fichiers d'identité des menaces (IDE) présents sur l'ordinateur, certaines caractéristiques du fichier (sa somme de contrôle et d'autres attributs) sont envoyées 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 sain ou malveillant, la décision est renvoyée à l'ordinateur et l'état du fichier est automatiquement mis à jour.
- Sélectionnez l'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, Sophos Live Protection permet à Sophos de demander un échantillon du fichier. Lorsque Sophos Live Protection est activée et si l'option **Envoyer automatiquement les échantillons de fichiers à Sophos** est activée et que Sophos n'a pas déjà d'échantillon de ce fichier, ce dernier est envoyé automatiquement. L'envoi de tels échantillons de fichiers aide Sophos à améliorer en permanence la détection des malwares sans aucun risque de faux positifs.

Important : assurez-vous que le domaine Sophos auquel les données des fichiers sont envoyées est fiable dans votre solution de filtrage Web. Retrouvez plus de renseignements dans l'article 62637 de la base de connaissances du support de Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/62637.aspx). Si vous utilisez une solution Sophos de filtrage Web, par exemple l'appliance Web WS1000, aucune intervention de votre part n'est nécessaire. Les domaines sont déjà fiables.

3. Détecter 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. Retrouvez plus de renseignements à la section Utilisation des contrôles planifiés à la page 36 ou Utilisation des contrôles planifiés à la page 36.
   b) Sélectionnez les options de nettoyage pour les virus/spywares.
4. Détecter les fichiers suspects.

   Les fichiers suspects contiennent certaines caractéristiques communes à celles des programmes malveillants mais pas suffisamment pour identifier le fichier comme un nouveau malware.

   a) Activez le contrôle sur accès ou planifiez un contrôle intégral du système pour détecter les fichiers suspects.
   b) Sélectionnez l'option **Fichiers suspects** dans les paramètres du contrôle.
   c) Sélectionnez les options de nettoyage des fichiers suspects.
   d) Autorisez, si nécessaire, tous les fichiers dont l'exécution est permise.
5. Détecter les comportements malveillants et suspects, les dépassements de la mémoire tampon et le trafic malveillant (surveillance des comportements).

Ces options surveillent en permanence les processus afin de déterminer si un programme manifeste un comportement malveillant ou suspect. Elles sont très utiles pour colmater les failles de sécurité.

a) Assurez-vous que la surveillance des comportements pour le contrôle sur accès est activée. Elle est activée par défaut.

b) Assurez-vous que l'option **Détecter le trafic malveillant** est sélectionnée.

c) 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.

d) Autorisez tous les programmes ou fichiers que vous souhaitez continuer à exécuter à l'avenir.

e) 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. Retrouvez plus de renseignements dans l'article 50160 de la base de connaissances du support de Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/50160.aspx).

6. Détecter les adwares et les PUA.

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

   Retrouvez plus de renseignements dans l'article 13815 de la base de connaissances du support de Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/13815.aspx).

7. Détecter les menaces dans les pages Web.

   Cette option bloque les sites connus pour héberger du contenu malveillant et contrôle les téléchargements à la recherche de contenu malveillant.

   a) Assurez-vous que l'option **Bloquer l'accès aux sites Web malveillants** est définie sur **Activé** pour bloquer les sites Web malveillants. Cette option est activée par défaut.

   b) Paramétrez l'option **Contrôle du contenu** sur **Activé** ou sur **Identique à celui sur accès** pour contrôler et bloquer toutes les 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.

   d) Assurez-vous que la réputation des fichiers est activée.

   Remarque : vous pouvez également utiliser la stratégie de contrôle du Web pour contrôler l'activité de navigation de vos utilisateurs en filtrant les sites Web à l'aide des 14 catégories répertoriant les principaux sites Web les plus inappropriés. Retrouvez plus de renseignements sur la manière de configurer la stratégie de contrôle du Web à la section Création de stratégies de contrôle du Web à la page 29.

Retrouvez plus de renseignements sur la création d'une stratégie antivirus et HIPS dans l'Aide de Sophos Enterprise Console.

5 Création de stratégies de pare-feu

5.1 À propos de la stratégie de pare-feu

La stratégie de pare-feu définit la manière dont le pare-feu assure la protection des ordinateurs. Seules les applications nommées ou les classes d'applications sont autorisées à accéder au réseau de l'entreprise ou à Internet.

Remarque : Sophos Client Firewall n'est pas pris en charge sur les systèmes d'exploitation serveur. Retrouvez plus de renseignements sur les configurations requises en matière de matériels et de systèmes d'exploitation sur la page Configuration requise du site Web de Sophos (http://www.sophos.com/fr-fr/products/all-system-requirements).

Attention : configurez la stratégie de pare-feu avant utilisation. Le déploiement d'une stratégie par défaut non modifiée dans un groupe via l'Enterprise Console entraînera des problèmes avec les communications réseau.

La stratégie de pare-feu par défaut n'est pas prévue pour un déploiement « tel quel » et n'est pas adaptée à une utilisation normale. Il s'agit d'une base pour vous aider à créer votre propre stratégie.

Par défaut, le pare-feu est activé et bloque tout le trafic réseau non indispensable. Tout ce qui n'a pas trait au réseau de base, par exemple, votre logiciel de messagerie, votre navigateur Web et tout accès réseau à la base de données, ne fonctionnera probablement pas correctement avec la stratégie par défaut qui bloque toutes les connexions non essentielles. Veuillez donc le configurer 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.

5.2 Planification des stratégies de pare-feu

Planifiez vos stratégies de pare-feu ainsi que ce que vous souhaitez qu'elles fassent avant de créer ou de modifier les règles de pare-feu (globale, application ou autre).

Lorsque vous planifiez vos stratégies de pare-feu, vous devez prendre en compte :

- Sur quels ordinateurs Sophos Client Firewall doit être installé ?
- Si un poste de travail est un ordinateur ou un portable. Il peut être judicieux de paramétrer un emplacement double pour les ordinateurs portables.
- Quelle méthode de détection de l'emplacement vous voulez utiliser, la recherche DNS ou la détection des adresses MAC à la passerelle.
- Les systèmes et protocoles réseau.
- Les connexions distantes.

D'après les applications et les droits d'accès réseau requis par les différents groupes d'utilisateurs, décidez combien de stratégies de pare-feu vous devez créer. Les stratégies couvrent différentes applications et varient en termes de restrictions. Sachez que plusieurs stratégies requièrent plusieurs groupes dans l'Enterprise Console.

- N'utilisez pas une seule stratégie Sophos Client Firewall. Vous seriez forcé d'ajouter des règles pour seulement un ou deux ordinateurs (par exemple, la station de travail de

l'administrateur) et ces règles seraient présentes sur l'ensemble du réseau. Ceci représente un risque pour la sécurité.

- Inversement, l'utilisation d'un grand nombre de configurations signifie du temps supplémentaire passé à la surveillance et à la maintenance.

Systèmes et protocoles réseau

Prenez en compte les services sur lesquels repose votre réseau. Par exemple :

- DHCP
- DNS
- RIP
- NTP
- GRE

Des règles existent dans la configuration du pare-feu par défaut pour couvrir la plupart de ces services. Par contre, sachez lesquels vous devez autoriser et ceux dont vous n'avez pas besoin.

Accès distant aux ordinateurs

Si vous utilisez un logiciel d'accès à distance pour surveiller et réparer les ordinateurs, créez dans votre configuration des règles qui vous permettront de fonctionner ainsi.

Identifiez les technologies que vous utilisez pour accéder aux ordinateurs sur votre réseau. Par exemple :

- RDP
- Client/serveur VPN
- SSH/SCP
- Terminal services
- Citrix

Vérifiez quelle sorte d'accès est nécessaire et créez vos règles en conséquence.

5.3 Paramètres conseillés

Lorsque vous créez votre stratégie de pare-feu, envisagez les actions suivantes :

- Lorsque Sophos Client Firewall est installé, le pare-feu Windows est désactivé. Par conséquent, si vous utilisiez le pare-feu Windows, notez les 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. En définissant d'abord une stratégie qui édite uniquement des rapports, vous aurez 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. L'Observateur d'événements est accessible en cliquant sur **Événements** > **Événements du pare-feu**.

- Examinez les règles créées via l'Observateur d'événements. Une application peut déclencher plusieurs événements de pare-feu (différents événements pour différentes actions effectuées par l'application), mais une règle d'application doit couvrir toutes les actions d'application. Par exemple, un client de messagerie peut déclencher deux événements différents lors de l'envoi et de la réception de messages alors qu'une règle d'application pour ce client doit gérer ces deux actions.
- Autorisez l'utilisation d'un navigateur Web, de la messagerie électronique et du partage de fichiers et d'imprimantes.
- Nous vous conseillons 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.
- N'utilisez pas le mode **Interactif** dans une stratégie où un emplacement double est configuré.
- N'utilisez pas le mode **Interactif** sur des réseaux de grande ou de moyenne taille et dans des environnements de domaine. Le mode **Interactif** peut être utilisé pour créer des règles de pare-feu sur de très petits réseaux (par exemple, jusqu'à 10 ordinateurs) dans des environnements de groupe de travail et sur des ordinateurs autonomes.

5.4 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 conseillons 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 conseillons 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 conseillons 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 configuration avancée de la stratégie de pare-feu, sur l'onglet **Général**, sous **Emplacement appliqué**, 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.

Attention : 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.

5.5 Déploiement d'une stratégie de pare-feu

Déployez une stratégie qui vous permette de surveiller tout le trafic passant par votre réseau. Vous recevrez des rapports de trafic dans l'Observateur d'événements du pare-feu. Utilisez ces informations pour paramétrer une stratégie de base.

Procédez au déploiement par phases de Sophos Client Firewall sur votre réseau. Déployez, par exemple, Sophos Client Firewall dans un groupe à la fois. Ainsi, vous éviterez de saturer votre réseau de trafic au cours des premières étapes.

Attention : tant que la configuration n'a pas été soigneusement vérifiée et testée, ne procédez pas au déploiement sur l'ensemble de votre réseau.

1. Déployez Sophos Client Firewall sur un groupe d'ordinateurs de test, représentatif des divers rôles sur votre réseau.
2. Configurez une stratégie de pare-feu pour utiliser le mode **Autoriser par défaut** afin de détecter (mais sans bloquer) le trafic, les applications et les processus habituels, et attribuez la stratégie au groupe test.

   a) Créez une nouvelle stratégie de pare-feu. Dans le volet **Stratégies** de l'Enterprise Console, cliquez avec le bouton droit de la souris sur **Pare-feu** et sélectionnez **Créer une stratégie**. Donnez un nom à cette stratégie, puis cliquez deux fois dessus.

      L'assistant de **Stratégie de pare-feu** apparaît.

   b) Choisissez d'utiliser l'assistant en cliquant sur **Suivant** ou de configurer la stratégie manuellement en cliquant sur **Stratégie de pare-feu avancée**.

      - À l'aide de l'assistant : cliquez sur **Suivant**. Sélectionnez **Emplacement unique** et cliquez sur **Suivant**. Sélectionnez **Surveiller**, cliquez sur **Suivant**, puis de nouveau sur **Suivant**, puis sur **Terminer**.
      - À l'aide de l'option **Stratégie de pare-feu avancée** : Dans la boîte de dialogue **Stratégie de pare-feu**, près de **Emplacement principal**, cliquez sur **Configurer**. Dans l'onglet **Général**, définissez le mode de fonctionnement sur **Autoriser par défaut**. Cliquez sur **OK**, puis de nouveau sur **OK**.

   c) Assignez la nouvelle stratégie de pare-feu au groupe test.

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. L'Observateur d'événements est accessible en cliquant sur **Événements** > **Événements du pare-feu**.

4. Surveillez les événements du pare-feu et créez votre stratégie sur une certaine période, par exemple, sur deux semaines.
   a) Créez des règles dans l'Observateur d'événements. Cliquez avec le bouton droit de la souris sur un événement pour lui créer une règle. Retrouvez plus de renseignements sur la création de règles dans l'Aide de Sophos Enterprise Console à la section *Configuration de stratégies* > *Stratégie de pare-feu*.
   b) Recherchez tous les points faibles éventuels de la stratégie (par exemple, un accès trop large attribué à certains utilisateurs).
   c) En cas de besoins différents, procédez à une sous-division du groupe et créez des stratégies et des règles supplémentaires si nécessaire.
5. Examinez les règles créées via l'Observateur d'événements. Une application peut déclencher plusieurs événements de pare-feu (différents événements pour différentes actions effectuées par l'application), mais une règle d'application doit couvrir toutes les actions d'application. Par exemple, un client de messagerie peut déclencher deux événements différents lors de l'envoi et de la réception de messages alors qu'une règle d'application pour ce client doit gérer ces deux actions.
6. Divisez le reste de votre réseau en groupes facilement administrables et représentatifs des multiples rôles sur un réseau, par exemple, stations de travail des commerciaux, stations de travail des administrateurs informatiques, etc..
7. Une fois que vous pensez tout couvrir, par exemple, lorsque vous n'obtenez plus de nouveaux événements de pare-feu pour lesquels il n'y a pas de règles, créez des stratégies à partir de vos règles et assignez-les selon les besoins. Si vous avez un nombre important d'ordinateurs sur votre réseau, nous vous conseillons de déployer Sophos Client Firewall sur un groupe à la fois.
8. Dès que vous avez testé les règles, changez le mode de stratégie sur **Bloquer par défaut**, sinon les ordinateurs demeureront non sécurisés.

Retrouvez plus de renseignements sur la création d'une stratégie de pare-feu dans l'Aide de Sophos Enterprise Console à la section *Configuration des stratégies* > *Stratégie de pare-feu*.

Remarque : comme alternative à la surveillance du trafic réseau et à la création de règles avec l'Observateur d'événements de pare-feu, sur un réseau de très petite taille ou sur des ordinateurs autonomes sous Windows 7 ou une version antérieure, vous pouvez installer Sophos Client Firewall sur un ordinateur de test et le configurer en mode **Interactif**. Lancez autant d'applications que possible sur votre réseau, y compris des navigateurs Web. Puis importez et modifiez la configuration du pare-feu contenant les règles établies par ce processus. Retrouvez plus de renseignements dans l'Aide de Sophos Endpoint Security and Control

6 Création de stratégies de contrôle d'applications

6.1 Paramètres conseillés

La stratégie de contrôle d'applications définit quelles applications sont bloquées et autorisées sur vos ordinateurs. Lorsque vous créez votre stratégie de contrôle d'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 d'applications afin de pouvoir vérifier l'utilisation des applications au sein de votre entreprise. L'Observateur d'événements est accessible en cliquant sur **Événements** > **Événements du contrôle d'applications**.
- Utilisez le Gestionnaire des rapports pour créer des rapports de tendance sur les événements de contrôle d'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 Déploiement d'une stratégie de contrôle d'applications

Par défaut, toutes les applications et tous les types d'applications sont autorisés. nous vous conseillons d'introduire le contrôle d'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 d'applications pour tout votre réseau.
3. Utilisez l'Observateur d'événements du contrôle d'applications pour voir quelles applications sont en cours d'utilisation et pour déterminer les applications ou les types d'application que vous souhaitez bloquer. L'Observateur d'événements est accessible en cliquant sur **Événements** > **Événements du contrôle d'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. Retrouvez plus de renseignements sur la création d'une stratégie de contrôle d'applications dans l'Aide de Sophos Enterprise Console.

Remarque : le contrôle d'applications peut être configuré pour bloquer CScript.exe qui est utilisé par la stratégie de correctif. Si vous utilisez à la fois la fonction de contrôle d'applications et la fonction de correctif, assurez-vous de ne pas bloquer **Microsoft WSH CScript** dans la catégorie **Outil de programmation/d'écriture de script**. Par défaut, les outils de programmation et d'écriture de script sont autorisés.

7 Création de stratégies de contrôle des données

7.1 Définition d'une 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 le stratégie de contrôle des données est activée, Sophos surveille l'activité de l'utilisateur à tous les points habituels de sortie des 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. Maintenue à jour par Sophos, la bibliothèque englobe un large nombre de formats de données personnelles identifiables et de données financières. 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.

7.2 Paramètres conseillés

Lorsque vous créez votre 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. L'Observateur d'événements est accessible en cliquant sur **Événements** > **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.

7.3 Déploiement d'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 conseillons 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 des 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 commande ne sont pas interceptés.

     Il est possible de forcer tous les transferts sur les périphériques de stockage surveillés qui sont à faire à l'aide de l'Explorateur Windows en utilisant l'action « Autoriser le transfert après accord de l'utilisateur et journaliser l'événement » ou 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 commande 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 commande 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 demeurent uniquement 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. Retrouvez plus de renseignements sur le contenu ou sur les actions contrôlés ou non contrôlés dans les applications 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 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 met à disposition une série d'exemple de règles que vous pouvez utiliser pour mettre au point votre stratégie de contrôle des données.

   Important : lors de la création de règles du contenu, sachez 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 conseillons 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 conseillons 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). L'Observateur d'événements est accessible en cliquant sur **Événements** > **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. À 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.

Retrouvez plus de renseignements sur la création d'une stratégie de contrôle des données dans l'Aide de Sophos Enterprise Console.

7.4 Principes du contrôle des données dans les applications

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

Retrouvez une liste complète des limites connues du contrôle des données dans l'article 63016 de la base de connaissances du support technique de Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/63016.aspx).

Applications	Actions de contrôle des données
Navigateurs Web	**Ce qui est contrôlé** ▪ Téléchargements de fichiers en amont ▪ Pièces jointes de messagerie Web ▪ Téléchargements Microsoft SharePoint en amont **Ce qui n'est pas contrôlé** ▪ Contenu des courriers de messagerie Web ▪ Entrées de blogs ▪ Téléchargements de fichiers

Applications	Actions de contrôle des données
	Remarque : dans un petit nombre de cas, les fichiers peuvent être contrôlés lorsqu'ils sont téléchargés.
Clients de messagerie	**Ce qui est contrôlé** ▪ Pièces jointes aux emails **Ce qui n'est pas contrôlé** ▪ Contenus des emails ▪ 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) ▪ Pièces jointes utilisant l'option « Envoyer ce fichier par courrier électronique » dans l'Explorateur Windows ▪ Pièces jointes copiées d'un email dans un autre email ▪ Pièce jointes enregistrées **Remarque :** dans un petit nombre de cas, les fichiers peuvent être contrôlés lorsqu'ils sont enregistrés.
Clients de messagerie instantanée	**Ce qui est contrôlé** ▪ Transferts de fichiers **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. **Ce qui n'est pas contrôlé** ▪ Contenu du message instantané ▪ Fichiers envoyés

8 Création de stratégies de contrôle des périphériques

8.1 Paramètres conseillés

La stratégie de contrôle des périphériques spécifie quels périphériques de stockage et de réseau sont autorisés à être utilisés sur les ordinateurs. Lorsque vous créez votre 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 **Bloqués** 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. L'Observateur d'événements est accessible en cliquant sur **Événements** > **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. Retrouvez une liste des périphériques de stockage amovibles sécurisés pris en charge dans l'article 63102 de la base de connaissances du support de Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/63102.aspx).
- 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 Wi-Fi) 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 ordinateur 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 d'utilisation, surtout ceux liés à la Wi-Fi et aux périphériques réseau.

Attention : 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 car l'ordinateur n'accepte aucune configuration supplémentaire depuis le serveur.

8.2 Déploiement d'une stratégie de contrôle des périphériques

Par défaut, le contrôle des périphériques est désactivé et tous les périphériques sont autorisés. Nous vous conseillons 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 **Bloqués** 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 quels périphériques sont en cours d'utilisation et pour déterminer les types de périphériques que vous souhaitez bloquer. L'Observateur d'événements est accessible en cliquant sur **Événements** > **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, vous pouvez ne pas vouloir autoriser l'accès des périphériques de stockage amovibles à vos services des ressources humaines et de finances, mais accepter 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 nombres d'alertes et de bloquer les périphériques dont vos utilisateurs pourraient avoir besoin. Retrouvez plus de renseignements sur la création d'une stratégie de contrôle des périphériques dans l'Aide de Sophos Enterprise Console.

9 Création de stratégies de protection antialtération

9.1 À propos de la stratégie de protection antialtération

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

Remarque : la protection antialtération n'est pas conçue pour assurer une protection contre les utilisateurs expérimentés techniquement. Elle n'assure pas la protection contre les programmes malveillants spécialement conçus pour corrompre le fonctionnement du système d'exploitation afin d'éviter d'être détecté. Ce type de malware sera uniquement détecté en effectuant un contrôle à la recherche de menaces et de comportements suspects. Retrouvez plus de renseignements à la section Création de stratégies antivirus et HIPS à la page 8.

Après avoir 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) du Panneau de configuration.

Lorsque vous créez 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. L'Observateur d'événements est accessible en cliquant sur **Événements** > **Événements de protection antialtération**.

9.2 Déploiement d'une stratégie de protection antialtération

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

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

   Le mot de passe permet uniquement aux utilisateurs de terminaux autorisés de reconfigurer, désactiver ou désinstaller le logiciel 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 sont généralement autorisés à effectuer, 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 différents groupes.

Retrouvez plus de renseignements sur la création d’une stratégie de protection antialtération dans l’Aide de Sophos Enterprise Console.

10 Création de stratégies de correctif

Remarque : cette fonction n'est pas incluse dans toutes les licences. Si vous voulez l'utiliser, il se peut que vous deviez personnaliser votre contrat de licence. Retrouvez plus de renseignements à la section https://www.sophos.com/fr-fr/products/endpoint-antivirus/how-to-buy.aspx.

10.1 À propos de la stratégie de correctif

La stratégie de correctif vous permet de vérifier que vos ordinateurs disposent des correctifs de sécurité les plus récents.

Les SophosLabs mettent à votre disposition des niveaux qui vous aident à déterminer quels sont les problèmes de correctifs de sécurité les plus sérieux afin que vous puissiez les résoudre rapidement. Les niveaux des SophosLabs prennent en compte les vulnérabilités les plus récentes et peuvent donc être différents du niveau de sévérité indiqué par un autre éditeur.

Lorsque vous créez votre stratégie de correctifs, utilisez l'Observateur d'événements d'évaluation des correctifs pour auditer les correctifs manquants sur les ordinateurs de votre entreprise. Vous allez y retrouver toutes les informations sur les correctifs de sécurité et les résultats des évaluations des correctifs. Si vous activez l'évaluation des correctifs dans la stratégie de correctif, vous pouvez voir l'état des correctifs par ordinateur, par groupe ou par menace. L'Observateur d'événements est accessible en cliquant sur **Événements** > **Événements d'évaluation des correctifs**.

Remarque : la fonction Correctif utilise CScript.exe qui pourrait être bloqué par le Contrôle d'applications. Si vous utilisez à la fois la fonction de contrôle d'applications et la fonction de correctif, assurez-vous de ne pas bloquer **Microsoft WSH CScript** dans la catégorie **Outil de programmation/d'écriture de script** dans la stratégie de **Contrôle d'applications**. Par défaut, les outils de programmation et d'écriture de script sont autorisés par le contrôle d'applications.

10.2 Déploiement d'une stratégie de correctif

Au départ, la stratégie de correctif « par défaut » est appliquée à tous les ordinateurs. L'évaluation des correctifs est désactivée dans la stratégie par défaut.

Dès que l'évaluation des correctifs est activée, celle-ci commence sur les ordinateurs. L'opération peut prendre quelques minutes. Les évaluations suivantes ont lieu aux intervalles définis dans la stratégie (par défaut, elles ont lieu tous les jours).

Remarque : si les ordinateurs commencent une évaluation avant que l'Enterprise Console ait téléchargé les données des correctifs depuis Sophos pour la première fois, l'observateur des événements des correctifs n'affichera aucun résultat. Le téléchargement peut durer quelques heures. Pour vérifier s'il est terminé, consultez le champ **Mises à jour des correctifs** dans la boîte de dialogue **Évaluation des correctifs - Observateur d'événements**.

Nous vous conseillons d’introduire la stratégie de correctif comme suit :

1. Déployez l’agent de correctif sur les ordinateurs à l’aide de l’Assistant de protection des ordinateurs. Sur la page **Sélection des fonctions** de l’assistant, sélectionnez **Correctif**.

   Remarque : vous devez impérativement protéger à nouveau les ordinateurs en exécutant l’Assistant de protection des ordinateurs si ceux-ci exécutent déjà Endpoint Security and Control sans l’agent de correctif.

2. Activez l’évaluation des correctifs dans votre stratégie de correctif par défaut.

   Vous avez, à présent, une stratégie de correctif pour tout votre réseau.

3. Utilisez l’Observateur d’événements d’évaluation des correctifs pour voir sur quels ordinateurs il manque des correctifs et lesquels sont à jour. L’Observateur d’événements est accessible en cliquant sur **Événements** > **Événements d'évaluation des correctifs**.

   Remarque : vous devez installer manuellement les correctifs manquants sur les ordinateurs.

4. Si vous avez besoin d’activer ou de désactiver la stratégie de correctif ou d’assigner différents intervalles d’évaluation des correctifs pour divers groupes, créez différentes stratégies pour différents groupes.

Retrouvez plus de renseignements sur la création d’une stratégie de correctif dans l’Aide de Sophos Enterprise Console.

11 Création de stratégies de contrôle du Web

Remarque : cette fonction n'est pas incluse dans toutes les licences. Si vous voulez l'utiliser, il se peut que vous deviez personnaliser votre licence. Retrouvez plus de renseignements à la section https://www.sophos.com/fr-fr/products/endpoint-antivirus/how-to-buy.aspx.

La stratégie de contrôle du Web spécifie les sites Web auxquels les utilisateurs peuvent accéder via leurs navigateurs Web.

Par défaut, le contrôle du Web est désactivé : les utilisateurs peuvent naviguer sur tous les sites non restreints dans le cadre de la protection Web de l'Enterprise Console. Vous pouvez utiliser la stratégie Contrôle des sites Web inappropriés ou la stratégie Contrôle intégral du Web. Les deux sont couvertes dans les sections qui suivent.

11.1 Paramètres conseillés

Vous pouvez choisir parmi deux stratégies différentes lors de la configuration du contrôle du Web : contrôle des sites Web inappropriés ou contrôle intégral du Web. En fonction de la stratégie que vous sélectionnez, les recommandations diffèrent. Lorsque vous créez votre stratégie de contrôle du Web, envisagez les actions suivantes :

Contrôle des sites Web inappropriés

- Examinez l'action pour chaque catégorie de sites Web et apportez des modifications en fonction de votre organisation ou de votre groupe. Pour accorder un accès Web différemment selon les multiples groupes d'ordinateurs, créez des stratégies différentes pour des groupes différents. Vous pourriez, par exemple, vouloir mettre des sites Web comme Facebook à la seule disposition du service des ressources humaines.
- Préparez une liste d'exemptions de sites Web avant de déployer une stratégie. Vous pouvez saisir manuellement les sites Web que vous voulez exclure de la stratégie à l'aide de l'onglet **Exceptions de site Web**. Par exemple, vous pouvez avoir une série d'adresses Web locales qui ne nécessitent aucun filtrage ou vous pouvez, si vous le souhaitez, bloquer les sites Web d'une catégorie autrement autorisée.
- Utilisez l'Observateur d'événements du contrôle du Web pour filtrer plus rapidement les événements que vous souhaitez consulter. L'Observateur d'événements est accessible en cliquant sur **Événements** > **Événements Web**. Vous pouvez, si vous le souhaitez, ajuster les paramètres de la catégorie de sites Web en fonction des actions affichées.

Contrôle intégral du Web

Important : vous devez avoir Sophos Web Appliance ou Security Management Appliance pour utiliser la stratégie de contrôle intégral du Web.

- Les guides de configuration de Sophos Web Appliance et de Security Management Appliance contiennent des instructions générales pour paramétrer votre appliance. L'appliance comporte un assistant de configuration pour vous assister dans le choix des paramètres les mieux adaptés à votre entreprise.

- Si vous le voulez, vous pouvez configurer des stratégies différentes suivant les types d'utilisateurs. Retrouvez plus de renseignements dans la documentation produit de Appliance Web disponible en ligne.

  Retrouvez toute la documentation de Sophos Web Appliance sur http://wsa.sophos.com/docs/wsa/.

- Avant de déployer une stratégie, planifiez toutes les exceptions à la stratégie de contrôle du Web. Vous pouvez, par exemple, utiliser la fonctionnalité « Heures spéciales » pour accorder tout l'accès ou une partie seulement à certains sites Web en dehors des heures de travail standard, comme lors du repas de midi. Vous pouvez aussi créer des « Stratégies supplémentaires » qui s'appliquent seulement à certains utilisateurs et qui sont des exceptions à la stratégie par défaut et à la stratégie Heures spéciales.
- Considérez quelle mesure (le cas échéant) vous voulez que Sophos Web Appliance prenne si les informations d'un site Web ne sont pas catégorisées. La case à cocher **Bloquer la navigation s'il est impossible de déterminer la catégorie du site Web** n'est ***pas*** sélectionnée par défaut. Cela signifie que les utilisateurs sont autorisés à continuer de naviguer si le service de catégorisation échoue. Lorsque la case à cocher est sélectionnée, les URL qui ne peuvent pas être catégorisées sont bloquées jusqu'à ce que le service soit restauré.

Retrouvez plus de renseignements dans la documentation de Sophos Enterprise Console et de Sophos Web Appliance.

11.2 Déploiement d'une stratégie de contrôle du Web

Pour commencer, vous devez décider du mode de filtrage Web à utiliser : contrôle des sites Web inappropriés ou contrôle intégral du Web. Vous devez avoir Sophos Web Appliance ou Security Management Appliance pour déployer la stratégie de contrôle intégral du Web.

Retrouvez plus de renseignements sur la création d'une stratégie de contrôle du Web dans l'Aide de Sophos Enterprise Console.

11.2.1 Déploiement d'une stratégie de contrôle des sites Web inappropriés

Cette option de base du contrôle du Web inclut 14 catégories de sites Web essentielles. Elle sert à empêcher les utilisateurs de visiter des sites Web inappropriés. Considérez les éléments suivants lors de la mise en place d'une stratégie de contrôle du Web. Retrouvez plus d'instructions spécifiques dans la documentation de l'Enterprise Console.

1. Assurez-vous que la stratégie de contrôle du Web est activée.
2. Si votre entreprise dispose d'une politique d'utilisation acceptable, personnalisez les paramètres en conséquence afin d'empêcher les utilisateurs de visiter des sites qui pourraient être jugés inappropriés.
3. Pour accorder un accès aux sites Web différemment selon les divers groupes d'ordinateurs, créez une stratégie différente pour chaque groupe.
4. Pensez aux groupes d'ordinateurs sujets au contrôle du Web et à quel type de stratégie convient à chaque groupe de machines.
5. Affichez l'action par défaut pour chaque catégorie de sites Web. Si vous préférez appliquer une action différente, sélectionnez-la dans la liste déroulante. Considérez les catégories que vous souhaitez bloquer aux utilisateurs, celles qui seront accessibles et celles à propos desquelles vous voulez avertir les utilisateurs.

6. Déterminez quels sites Web vous voulez exempter du filtrage et ajoutez-les à la liste **Sites Web à autoriser** ou **Sites Web à bloquer**.

   Remarque : en cas de conflits entre les entrées ou si elles apparaissent à la fois dans les listes « Bloquer » et « Autoriser », ce sont les entrées de la liste Bloquer qui sont prises en compte. Par exemple, si la même adresse IP apparaît dans la liste Bloquer et dans la liste Autoriser, le site Web est bloqué. De plus, si un domaine est inclus à la liste Bloquer et qu'un sous-domaine de ce domaine est inclus à la liste Autoriser, l'entrée Autoriser est ignorée et le domaine et tous ses sous-domaines sont bloqués.

7. Utilisez l'Observateur d'événements du contrôle du Web pour examiner les résultats du filtrage. L'Observateur d'événements est accessible en cliquant sur **Événements** > **Événements Web**. Utilisez l'Observateur d'événements pour voir les événements Web. En fonction de ces résultats, vous pouvez, si vous le souhaitez, faire des ajustements.

Retrouvez plus de renseignements dans la documentation de l'Enterprise Console.

11.2.2 Déploiement d'une stratégie de contrôle intégral du Web

Ce mode utilise une stratégie Web complète. Elle applique une stratégie de contrôle du Web complète dotée d'un maximum de fonctions et fournit des rapports complets sur le trafic Web. Sophos Web Appliance ou Security Management Appliance est requise pour cette option.

1. Configurez votre Sophos Web Appliance ou votre Security Management Appliance comme le décrit la documentation de l'appliance en vous assurant que l'option **Endpoint Web Control** est activée.
2. Assurez-vous que le contrôle du Web est activé sur l'Enterprise Console.
3. Si votre entreprise dispose d'une politique d'utilisation acceptable, personnalisez les paramètres en conséquence afin d'empêcher les utilisateurs de visiter des sites qui pourraient être jugés inappropriés.
4. Pour accorder l'accès aux sites Web différemment selon les divers groupes d'utilisateurs, créez une stratégie différente pour chaque ensemble d'utilisateurs.
5. Déterminez quels sites Web vous voulez contrôler. Quelles catégories souhaitez-vous empêcher les utilisateurs de visiter ? Quelles catégories seront accessibles ? À propos de quelles catégories de sites Web souhaitez-vous avertir les utilisateurs ?
6. Déterminez les sites Web à exempter et ajoutez-les à la liste des site locaux (Local Site List) de l'appliance.
7. Avec le contrôle intégral du Web, vous avez la possibilité d'utiliser Sophos LiveConnect. Vous pouvez configurer l'appliance pour l'utilisation de LiveConnect afin que les mises à jour de stratégies soient distribuées aux utilisateurs et que les données de signalement depuis les machines des utilisateurs soient téléchargées en amont, même s'ils ne sont pas connectés depuis le réseau.

Retrouvez plus de renseignements dans la documentation de Sophos Enterprise Console et de Sophos Web Appliance.

12 Création des stratégies de prévention des Exploits

Remarque : cette fonction n'est pas incluse dans toutes les licences. Si vous voulez l'utiliser, il se peut que vous deviez personnaliser votre contrat de licence. Retrouvez plus de renseignements à la section https://www.sophos.com/fr-fr/products/endpoint-antivirus/how-to-buy.aspx.

La stratégie de prévention des Exploits indique le niveau de protection contre les ransomwares et contre toutes autres formes d'exploitation par les malwares.

- Protéger les fichiers document contre les ransomwares (CryptoGuard).
- Protéger les fonctions critiques des navigateurs Web (Safe Browsing).
- Limiter les attaques d'exploitation des failles de sécurité. Cette option permet de protéger les applications les plus vulnérables aux attaques de malwares (par exemple, les applications Java).
- Protéger contre les attaques contre les processus creux.
- Protéger contre le chargement de fichiers .DLL à partir de dossiers non fiables.
- Protéger contre la surveillance d'exécution du processeur.

12.1 Paramètres conseillés

La stratégie de prévention des Exploits comment le logiciel de sécurité assure la protection contre les ransomwares et contre toutes autres formes d'exploitation par les malwares.

Remarque : par défaut, toutes les options de prévention des Exploits sont activées.

Nous vous conseillons d'utiliser les paramètres par défaut.

12.2 Déploiement d'une stratégie de prévention des Exploits

Nous vous conseillons de déployer la stratégie de prévention des Exploits comme suit :

1. Par défaut, toutes les options de prévention des Exploits sont activées. Nous vous conseillons d'utiliser les paramètres par défaut. Veuillez surveiller tous les événements de prévention des Exploits pendant une certaine période de temps avant de modifier les paramètres.
2. Utilisez l'Observateur d'événements de la prévention des Exploits pour surveiller tous les événements de prévention des Exploits. L'Observateur d'événements est accessible en cliquant sur **Événements** > **Événements de prévention des Exploits**.
3. Modifiez la stratégie de prévention des Exploits selon votre méthode de surveillance. Vous pourriez par exemple souhaitez exclure certaines applications de l'atténuation de l'exploitation des failles de sécurité. Retrouvez plus de renseignements dans l'Aide de Sophos Enterprise Console à la section *Configuration des stratégies* > *Stratégie de prévention des Exploits*.

Important : les applications vulnérables sont protégées par défaut. Veuillez procéder à l'exclusion d'applications de la prévention des Exploits avec le plus grand soin. Veuillez noter qu'elles demeureront protégées par CryptoGuard et Safe Browsing.

a) Créez une nouvelle stratégie ou modifiez la stratégie par défaut.

b) Recherchez tous les points faibles éventuels de la stratégie.

c) En cas de besoins différents, procédez à une sous-division du groupe et créez des stratégies supplémentaires si nécessaire.

4. Assignez vos stratégies de manière adéquate.

Retrouvez plus de renseignements sur la création de stratégies de prévention des Exploits dans l'Aide de Sophos Enterprise Console.

13 Conseils à suivre pour le contrôle

Les options de contrôle dans les sections suivantes sont définies dans la stratégie antivirus et HIPS. Lors du choix des options de contrôle, envisagez les actions suivantes :

- Utilisez les paramètres par défaut à chaque fois que c'est possible.
- Définissez le contrôle dans l'Enterprise Console ainsi que sur l'ordinateur lui-même, si possible.
- Prenez en compte le rôle de l'ordinateur (par exemple, ordinateur de bureau ou serveur).

Extensions

Pour accéder aux options d'extension pour le contrôle sur accès, dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur **Configurer** près de **Activer le contrôle sur accès**, puis allez sur l'onglet **Extensions**.

Pour les contrôles planifiés, dans la boîte de dialogue **Stratégie antivirus et HIPS**, sous **Contrôle planifié**, cliquez sur **Extensions et exclusions**.

- Généralement, l'option **Contrôler tous les fichiers** n'est ni nécessaire ni 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.

Autres options de contrôle

Pour accéder aux autre options de contrôle sur accès, dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur **Configurer** près de **Activer le contrôle sur accès**.

Pour les contrôles planifiés, dans la boîte de dialogue **Stratégie antivirus et HIPS**, sous **Contrôle planifié**, sélectionnez un contrôle et cliquez sur **Modifier**. Dans la boîte de dialogue **Paramètres du contrôle planifié**, cliquez sur **Configurer**.

- L'option **Contrôler dans les fichiers archive** ralentit le contrôle et n'est généralement pas nécessaire. Lorsque vous tentez d'accéder au contenu d'un fichier archive, ce fichier est contrôlé automatiquement. Par conséquent, nous vous conseillons de ne pas sélectionner cette option sauf si vous utilisez fréquemment des fichiers archive.
- Nous vous conseillons 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 activée par défaut.

14 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.
- Les options **À la lecture**, **À l'écriture** et **Au moment de renommer** du contrôle sur accès sont activées par défaut uniquement sur les nouvelles installations du logiciel. Pour les mises à niveau du logiciel, vous devez activer ces options.
- 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. Retrouvez plus de renseignements sur l'utilisation de la stratégie antivirus et HIPS avec un logiciel de chiffrement dans l'article 12790 de la base de connaissances Sophos.
- Si vous ne sélectionnez pas le contrôle sur accès, assurez-vous que les ordinateurs utilisent les contrôles planifiés. Retrouvez plus de renseignements à la section Utilisation des contrôles planifiés à la page 36.

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

15 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.
- 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 minimes sur les applications de l'utilisateur. Cette option est conseillée, même si le contrôle prendra plus de temps.

16 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.

17 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 du contrôle des éléments spécifiques, tels que les fichiers ou les lecteurs. 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 conseillons 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.

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

18 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum Sophos Community en anglais sur 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 www.sophos.com/fr-fr/support.aspx.
- Téléchargez la documentation des produits sur www.sophos.com/fr-fr/support/documentation.aspx.
- Ouvrez un incident support sur https://secure2.sophos.com/fr-fr/support/contact-support/support-query.aspx.

19 Mentions légales

Copyright © 2009–2017 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 documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos, Sophos Anti-Virus et SafeGuard sont des marques déposées de Sophos Limited, Sophos Group et de Utimaco Safeware AG, partout où ceci est applicable. Tous les autres noms de produits et d'entreprises mentionnés dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™ (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (c) 1993-2014, all rights reserved. Since DOC software is open-source, freely available software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with any code built using DOC software that you release. No copyright statement needs to be provided if you just ship binary executables of your software products.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not misappropriate the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, in a way that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us know so we can promote your project in the DOC software success stories.

The ACE, TAO, CIAO, DAnCE, and CoSMIC web sites are maintained by the DOC Group at the Institute for Software Integrated Systems (ISIS) and the Center for Distributed Object Computing of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter "as is" with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use,

correction, modification, or enhancement. A number of companies around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at http://www.apache.org/licenses/LICENSE-2.0

Boost Software License

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Common Public License

The Sophos software that is referenced in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source

code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.fr or via the web at https://www.sophos.com/fr-fr/support/contact-support.aspx. A copy of the license agreement for any such included software can be found at 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.

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Microsoft Public License (MS-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

   The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

   A "contribution" is the original software, or any additions or changes to the software.

   A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

   (A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

   (B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

   (A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

   (B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

   (C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

   (D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

   (E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

A copy of the MS-PL terms can be found at https://opensource.org/licenses/MS-PL.

OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2016 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Windows Template Library (WTL)

Copyright © Microsoft Corporation. All rights reserved.

The use and distribution terms for this software are covered by the Common Public License. Source code for this component is available here: https://sourceforge.net/projects/wtl/files/

zlib data compression library

Copyright © 1995–2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu