KASPERSKY lab

GUIDE DES BONNES PRATIQUES

Technologies de contrôle des terminaux

www.kaspersky.fr

VOTRE GUIDE DES BONNES PRATIQUES EN MATIÈRE DE CONTRÔLE DES TERMINAUX.

Le cyber-espionnage et les menaces soutenues par des États ont fait la une des journaux récemment, mais le fait est que la même technologie peut et sera utilisée à l'encontre d'entreprises comme la vôtre.

Vous ne pouvez pas bloquer Internet et vous ne pouvez pas voir tout ce qui se passe sur votre réseau en temps réel, mais vous avez un pouvoir de gestion et de contrôle. Vous pouvez parfaitement contrôler ce qui se passe lorsqu'un utilisateur clique là où il ne devrait pas cliquer ou installe quelque chose qu'il ne devrait pas installer. Voici la marche à suivre...

1. NE VOUS CONTENTEZ PAS DE BLOQUER, CONTRÔLEZ

Les médias sociaux, les appareils intelligents, les applications basées sur Internet, les courriers indésirables, le phishing, les sites Web malveillants, l'ingénierie sociale, les programmes malveillants... Il devient de plus en plus difficile pour les responsables informatiques de rester informés des menaces de plus en plus complexes qui traversent des frontières de plus en plus floues.

Et il ne s'agit là que des risques extérieurs à votre entreprise. Que dire de l'activité de l'utilisateur final qui expose votre entreprise aux violations de données et autres atteintes à la sécurité ? Codes malveillants incorporés aux jeux en ligne, liens dangereux dans les applications de réseaux sociaux, programmes malveillants cachés dans des documents apparemment inoffensifs... Aujourd'hui, les criminels exploitent les vulnérabilités associées aux utilisateurs individuels pour accéder aux réseaux professionnels et aux données sensibles qu'ils contiennent.

Le contrôle des applications, des appareils et du Web, associé à de solides technologies de lutte contre les programmes malveillants, peut protéger votre entreprise sans nuire à la productivité ni à la flexibilité. Prenez le contrôle de vos technologies en appliquant ces contrôles faciles à mettre en œuvre.

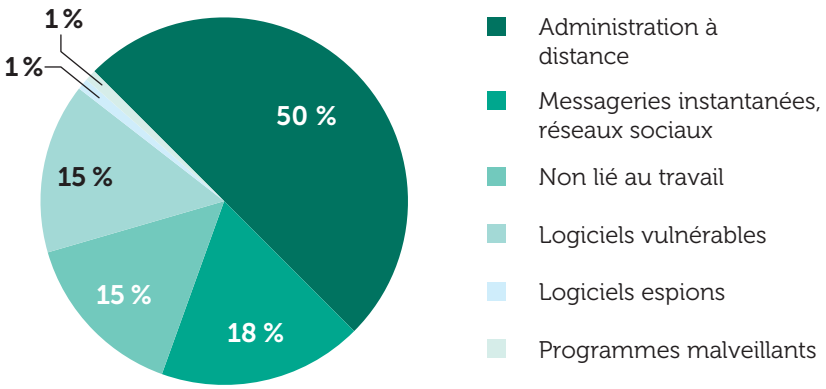
Prenez garde aux applications

Dans un monde hyperconnecté, les vulnérabilités des applications Web sont désormais la porte d'entrée privilégiée des cyber-criminels. Rien qu'en 2014, Kaspersky Lab a détecté et neutralisé plus de **6,2** milliards d'attaques lancées à partir de ressources en ligne à l'échelle mondiale[1], contre **1,7** milliard en 2013[2]. Ces attaques ont été lancées par **9,7** millions d'ordinateurs hôtes différents[3]. Chaque jour, Kaspersky Lab détecte quelque **325 000** nouveaux fichiers malveillants[4].

Dans la mesure où un téléchargement sur **14** contient des programmes malveillants[5], bloquer simplement les téléchargements ne vous permettra pas d'aller bien loin... Chaque jour, des criminels lancent des programmes malveillants pour exploiter les vulnérabilités de logiciels professionnels légitimes : les applications tierces représentent en moyenne **75** % des vulnérabilités[6].

1 Bulletin de Kaspersky Lab sur la sécurité 2014
2 Bulletin de Kaspersky Lab sur la sécurité 2013
3 Bulletin de Kaspersky Lab sur la sécurité 2014
4 Bulletin de Kaspersky Lab sur la sécurité 2014
5 Bulletin de Kaspersky Lab sur la sécurité 2014
6 Analyse des vulnérabilités de Secunia 2014

La réalité pour les professionnels de la sécurité informatique est que le maillon faible de la chaîne de sécurité est le plus souvent déjà présent dans leurs systèmes, ou se trouve face à eux.



2. CONTRÔLE DES APPLICATIONS ET LISTE BLANCHE : LAISSEZ LES MENACES À L'EXTÉRIEUR, PRÉVENEZ LES ATTEINTES À LA SÉCURITÉ

Les technologies de contrôle des applications et de liste blanche dynamique contribuent à protéger les systèmes des menaces connues et inconnues. Les administrateurs ont en effet un contrôle total sur les types d'applications et de programmes pouvant être exécutés sur leurs terminaux, indépendamment du comportement des utilisateurs.

En fait, les contrôles des applications vous permettent de créer et d'appliquer des règles de sécurité et des politiques d'utilisation de manière plus efficace :

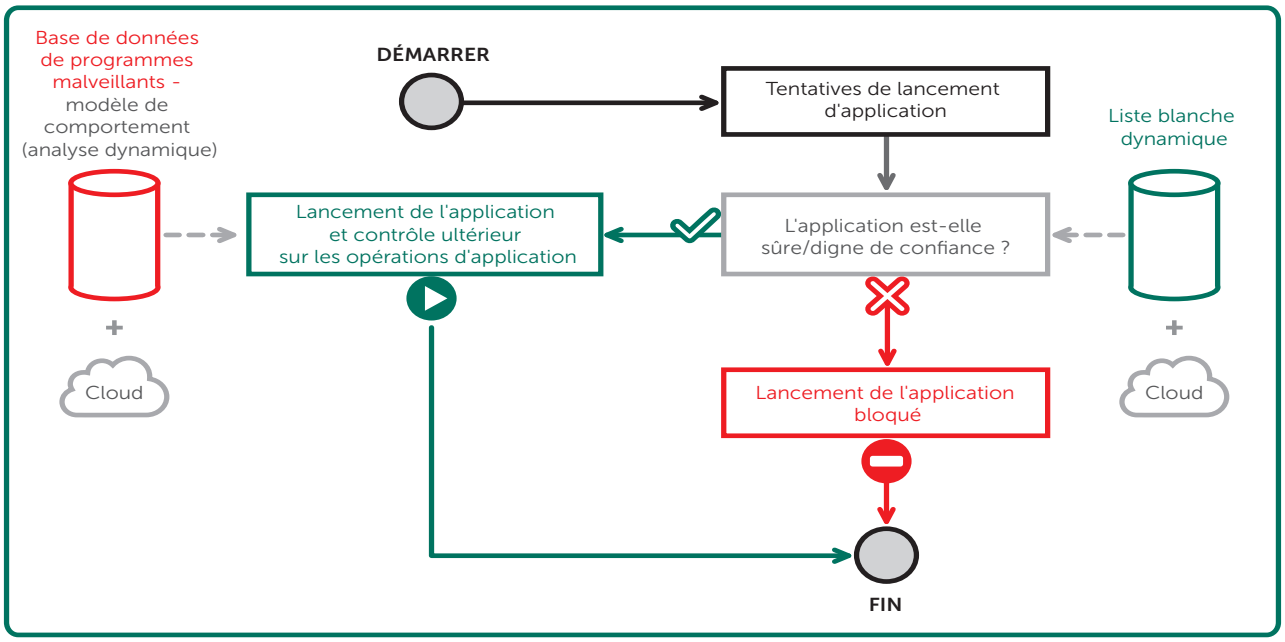
- **Contrôle au démarrage des applications** : autorisation, blocage et vérification des démarrages d'applications. Améliore la productivité puisque l'accès aux applications non professionnelles est restreint.
- **Contrôle des privilèges des applications** : régulez et contrôlez l'accès des applications aux ressources et données système, classez les applications en catégories (fiables, non fiables ou accès restreint).
- **Recherche des vulnérabilités des applications** : permet d'appliquer une défense proactive contre les attaques ciblant les vulnérabilités des applications de confiance.
- **Surveillance des applications** : en plus de pouvoir bloquer ou autoriser certaines applications, vous pouvez contrôler leur comportement, les ressources qu'elles utilisent, les types de données auxquelles elles accèdent ou qu'elles modifient, leur capacité à écrire dans les registres, etc. Autrement dit, vous pouvez empêcher toute application d'exécuter certaines actions représentant un risque pour le terminal et le réseau auquel il est connecté.

  Vous savez ainsi en permanence et en temps réel qui accède aux applications et comment, ce qui vous permet de dégager des tendances d'utilisation. Ces données vous aideront ensuite à mieux définir vos politiques en fonction des exigences et des menaces propres aux différents utilisateurs.

Liste blanche – contrôle et robustesse au cœur du système

Si le contrôle des applications est le véhicule d'une protection efficace contre les menaces complexes, la liste blanche dynamique en est le moteur. La liste blanche est en fait un élément incontournable de toute stratégie efficace de contrôle des applications. Pour faire court : sans liste blanche, pas de véritable contrôle des applications.

Les listes blanches répertorient les applications fiables et permettent de renforcer la sécurité des contrôles existants en ajoutant une couche de protection. Chaque fois qu'une application tente de s'exécuter, le système consulte la liste blanche. Si l'application y figure, l'exécution est autorisée conformément aux règles et politiques définies par l'administrateur. Si elle n'y figure pas, l'exécution est bloquée jusqu'à l'approbation de l'administrateur. C'est comme si votre terminal disposait d'un portier ou d'un concierge.



Envisagez d'adjoindre à la liste blanche une approche de blocage par défaut

Le blocage par défaut est la mesure de sécurité la plus efficace face aux menaces en constante évolution. Avec cette approche, l'exécution de toutes les applications est bloquée sur n'importe quel poste de travail. Seules les applications autorisées par l'administrateur peuvent être directement exécutées.

Sous ses airs de stratégie un peu brutale qui ne vous vaudra pas que des amis au sein de l'entreprise, le blocage par défaut basé sur une liste blanche efficace offre toutefois une certaine flexibilité à vos utilisateurs.

L'objectif n'est pas de tout bloquer, mais bien de décider avec précision ce que vous autorisez.

La meilleure façon de déterminer l'impact d'un scénario de blocage par défaut sur votre entreprise est de l'essayer. L'utilisation d'une sandbox vous permettra d'observer les effets réels de la mise en œuvre de cette approche sur votre système informatique, et de tester les ajustements nécessaires, sans aucune perturbation sur vos systèmes ou vos utilisateurs. Vous serez sans doute surpris, lorsque vous la mettrez à l'essai, du peu d'impact que cette approche a sur vos utilisateurs en pratique.

Utilisez les bases de données de liste blanche

Vous avez donc décidé de travailler avec une liste blanche. Mais vous avez autre chose à faire que de compiler, réviser et mettre à jour des listes d'applications « sûres ». Car le but n'est pas de contrôler simplement quelques applications. Il faut aussi penser aux pilotes d'imprimante, aux logiciels d'infrastructure réseau ou encore aux mises à jour.

Les solutions les plus efficaces s'appuient sur des bases de données de liste blanche dynamiques et automatiques, surveillées et mises à jour en permanence. Rassurés de savoir que ces bases de données fonctionnent en arrière-plan, les administrateurs peuvent ainsi se concentrer sur leur travail.

Autres outils utiles

Une solution efficace de liste blanche et de contrôle des applications vous permet d'appliquer les meilleures pratiques de mise en œuvre, sans devoir sélectionner manuellement les centaines de logiciels utilisés par les entreprises (même les plus petites) dans leurs activités quotidiennes. Un bon programme est celui qui vous facilite non seulement la vie, mais inclut également des fonctions clés inspirées des meilleures pratiques, parmi lesquelles :

- **Inventaire** : parce que pour évaluer ou surveiller quelque chose, il faut déjà savoir ce qu'on a. Les meilleurs programmes de liste blanche commencent donc par proposer une fonction d'inventaire, qui permet de dresser et de mettre à jour une liste des logiciels installés sur le réseau, dans un format pratique facilitant les analyses. Pour vous simplifier la vie, optez pour une solution qui propose un inventaire automatique. Vous gagnerez du temps et vous vous épargnerez la peine de répertorier chaque logiciel utilisé dans votre entreprise. L'inventaire automatique permet en plus de repérer les applications indésirables.

- **Catégorisation** : classez vos logiciels installés en catégories fonctionnelles (systèmes d'exploitation, logiciels professionnels, outils de développement, périphériques, navigateurs, multimédia, etc.). Les administrateurs peuvent ainsi identifier plus facilement les applications professionnelles et bloquer les applications qui nuisent à la productivité des employés. Utilisées intelligemment, ces catégories permettent par exemple de bloquer purement et simplement tous les jeux auxquels jouent les utilisateurs pendant leur temps de travail. Si jamais ils détectent un programme méconnu passé entre les mailles du filet, les administrateurs peuvent toujours l'ajouter à la liste. Leurs essais exploratoires du blocage par défaut peuvent par ailleurs les conduire à créer de nouvelles catégories en fonction des résultats de leurs recherches.

- **Mises à jour de confiance** : effectuez des mises à jour régulières des logiciels autorisés, pour bloquer les vulnérabilités nouvelles ou non détectées auparavant. Cela inclut les correctifs, les processus de gestion des systèmes et autres programmes de développement logiciel.

- **Mise en œuvre de règles souples** : les solutions de qualité intègrent un large spectre de règles prédéfinies répondant aux scénarios les plus fréquents. Si elles sont indispensables à votre fonctionnement au début, en attendant que votre liste blanche soit parfaitement en place et exhaustive, vous aurez certainement envie de personnaliser vos paramètres pour les adapter au contexte propre à votre entreprise.

  Vous avez besoin d'options basées sur des facteurs tels que nom de fichier, dossier source ou fournisseur, alors ne vous limitez pas à une solution qui offre peu de flexibilité en matière de personnalisation. La flexibilité en matière de hachage MD5 (empreinte numérique des données) est également importante. Cette technique empêche les cyber-criminels (ou plutôt les employés rusés) de contourner votre liste blanche en faisant passer des applications et fichiers interdits pour des applications et fichiers autorisés.

- **Pensez global, agissez local**

  Vous devez toujours travailler à partir d'une base de données de liste blanche mondiale complète et dynamique. Parce que vous n'avez ni le temps ni les ressources pour la créer vous-même, la base de données de liste blanche de Kaspersky Lab contient par exemple plus de 500 millions de fichiers uniques.

  Sur une journée classique, Kaspersky Lab charge plus d'un million de fichiers, ce qui est assez pour occuper tout un service dédié aux listes blanches. Les bases de données mondiales doivent être disponibles et accessibles en permanence dans le cloud. Les fournisseurs des grandes applications professionnelles sortent sans cesse de nouvelles mises à jour et versions de leurs produits ; la mise à jour régulière des bases de données mondiales permet ainsi de réduire le risque de faux positifs.

  Vous pouvez admettre la nécessité des bases de données mondiales sans pour autant en oublier de personnaliser votre propre liste blanche entièrement locale, uniquement applicable à votre réseau. Optez pour une solution qui vous le permet, en particulier si vous développez vos propres applications personnalisées.

- **Visez l'or**

  Une « Golden Image » est votre modèle de la parfaite installation : toutes les applications et tous les paramètres vitaux de votre entreprise mis en œuvre conformément aux meilleures pratiques et affinés pour fonctionner à un niveau de performance optimal.

  Dans la pratique, les professionnels informatiques ont très rarement l'opportunité de partir de zéro. Mais que vous partiez de machines flambant neuves qui n'ont encore jamais été connectées à Internet ou que vous deviez progressivement modifier et ajuster votre liste blanche en vous appuyant sur des technologies préexistantes, vous devez développer votre « Golden Image ». Que votre Golden Image soit pour vous un point de référence pour développer au fur et à mesure votre programme de contrôle des applications, ou une plateforme de base pour votre stratégie de blocage par défaut, tournez-vous vers une solution qui vous aide à créer et à développer ce modèle. Votre vie en sera grandement simplifiée. Surtout si la solution fournit un modèle « mondial » prêt à l'emploi.

Liste blanche ou noire ? Les deux !

La liste blanche autorise uniquement l'exécution des applications pré-approuvées, contrairement au traditionnel antivirus (fonctionnant sur le principe de la « liste noire »), qui bloque les logiciels une fois qu'ils ont été identifiés comme malveillants. En réunissant sous le même toit la liste blanche et la liste noire, vous barricadez efficacement toute votre maison, les portes de derrière comme les portes de devant.

L'association de ces deux technologies complémentaires offre une protection multiniveaux inspirée des meilleures pratiques pour une sécurité optimale. La liste blanche peut même améliorer les performances de votre antivirus. En effet, les applications de la liste blanche ne requièrent pas le même niveau de contrôle que les autres, ce qui permet d'économiser des ressources système et de gagner en performances.

3. LA QUESTION DU CONTRÔLE DES APPAREILS

Maintenant que vous savez que vous pouvez contrôler les applications qui peuvent être exécutées ou non sur vos terminaux, il vous faut bénéficier du même niveau de contrôle sur les appareils.

Réduisez de manière significative le risque venant de l'intérieur de votre entreprise en centralisant les politiques entourant l'utilisation des appareils et supports amovibles (clés USB, disques durs à mémoire flash, lecteurs de CD/DVD, cartes à puce...). Que vous soyez préoccupé par un employé mécontent copiant des données sensibles sur une clé USB ou que vous souhaitiez tout simplement empêcher les appareils portables infectés de se connecter à votre terminal ou réseau, le contrôle des appareils propose une approche souple pour ces opérations.

Voici quelques notions importantes à considérer lorsque vous adoptez un programme de contrôle des appareils :

- **Définissez vos catégories** : les différents appareils n'ont pas les mêmes capacités et ne représentent donc pas les mêmes menaces. L'approche du blocage par défaut convient naturellement, par exemple, pour un scanner d'images. Mais en désactivant un port USB, vous empêchez également l'utilisation de ce port pour un accès VPN sécurisé avec jeton. C'est pourquoi vous avez besoin de ce qui suit...
- **Granularité** : vous devez être en mesure d'établir différentes règles pour différents appareils et même différents utilisateurs et cas d'utilisation. Les administrateurs doivent pouvoir appliquer des politiques (lecture seule, blocage, lecture, écriture, etc.) à différents appareils.

  Cette granularité doit également vous permettre de définir les types de fichiers transférables, les horaires auxquels appliquer telle ou telle politique, le type d'appareil autorisé et quand. Votre tâche sera beaucoup plus facile si vous pouvez appliquer ces règles simultanément à de multiples appareils.

  Pour un contrôle encore plus poussé, vous devez avoir la possibilité d'appliquer une politique au numéro de série précis de n'importe quel appareil. Vous pouvez ensuite définir des politiques et des autorisations pour des modèles d'appareils et des utilisateurs particuliers, de manière à empêcher les autres employés d'accéder aux données de ces appareils.
- **Contrôle d'accès** : cette fonction offre un contrôle total de l'accès à des types d'appareils particuliers pour des utilisateurs et groupes sélectionnés, pendant des périodes spécifiques. Elle peut être utile si vous cherchez, par exemple, à réduire les coûts sur les impressions en dehors des horaires de travail.

- **Chiffrement** : les meilleures pratiques en matière de gestion des appareils incluent un élément de chiffrement. Nous savons tous que les clés USB se perdent ou sont volées facilement. Des politiques peuvent être définies pour imposer le chiffrement sur certains types d'appareils.
- **Intégration avec Active Directory** : plutôt que de courir après chacun de vos utilisateurs dans l'entreprise afin d'appliquer vos politiques, définissez simplement les politiques de contrôle des appareils et déployez-les sur les postes de vos utilisateurs.

4. ÊTES-VOUS SEUL ?

Une dernière question : qui va faire tout cela ? Est-ce vous ? Est-ce là l'intégralité de vos responsabilités dans le domaine informatique ? La gestion des contrôles, ou de la sécurité en général, ne représente sans doute qu'une partie de votre travail, bien que nous espérions que votre entreprise reconnaisse, tout autant que nous, l'importance de cet aspect de votre travail.

Si vous êtes seul, ou faites partie d'une petite équipe, vous devez être en mesure de contrôler la sécurité en général à partir d'un seul écran, sans passer d'une console à une autre.

Vous pouvez aussi faire partie d'une grande équipe de sécurité, auquel cas votre domaine de responsabilité ne couvre qu'un seul aspect, tel que la gestion des appareils. Dans ce cas, vous avez besoin d'un système de sécurité qui incorpore un contrôle des accès basé sur les rôles (RBAC), pour que vous puissiez seul contrôler la sécurité de cet aspect.

Mais vous ne devriez pas avoir à choisir. Il n'y a aucune raison pour que les mêmes contrôles de sécurité ne soient pas facilement gérables par un individu surchargé ou par différents membres d'une équipe extrêmement sollicitée. C'est une question d'intégration. Un système de sécurité dont tous les éléments, y compris les contrôles, travaillent de concert dans le cadre d'une seule et même plateforme, ne peut-être qu'une bonne chose.

POUR FINIR...

Dans un contexte où les menaces évoluent en permanence, les entreprises ne peuvent plus se contenter de bloquer les programmes malveillants et autres menaces une fois ceux-ci détectés. La technologie efficace de la liste noire a toujours sa place dans la stratégie sécuritaire, mais une protection totale passe forcément par une approche multiniveaux.

Vous devez protéger votre entreprise des programmes malveillants classiques, mais aussi des menaces provenant de sources légitimes : les vulnérabilités des applications fiables, les codes malveillants intégrés aux sites Internet populaires, les attaques de phishing par e-mail ou encore les programmes malveillants conçus pour exploiter les fonctions d'exécution automatique des périphériques portables.

La base de données mondiale de liste blanche de Kaspersky Lab est ce qu'il se fait de mieux : nous sommes la seule entreprise de sécurité informatique à avoir un laboratoire spécialisé dans les listes blanches, avec sa propre équipe d'experts dédiés. Le tout à partir d'une plateforme unique pour un contrôle centralisé et une efficacité optimale.


Twitter.com/
KasperskyFrance


Facebook.com/
KasperskyLabFrance


Youtube.com/
KasperskyFrance

Kaspersky Lab, Moscou, Russie
www.kaspersky.fr

Tout savoir sur la sécurité sur Internet :
www.securelist.com
http://www.viruslist.com/fr/

Rechercher un partenaire près de chez vous :
http://www.kaspersky.fr/partners/buyoffline/liste-des-partenaires

KASPERSKY lab