McAfee Application and Change Control

Protection complète contre les modifications non sollicitées ou le contrôle non autorisé des applications, des terminaux, des serveurs et des équipements à fonction fixe

Face à des menaces APT exécutées par attaque à distance ou ingénierie sociale, il est de plus en plus difficile de protéger les entreprises, ce qui peut entraîner des compromissions de sécurité, des fuites de données et des pannes. Les modifications malveillantes peuvent facilement passer inaperçues, en particulier dans les environnements de serveurs et de cloud actuels, en constante évolution. Le logiciel McAfee® Application and Change Control est la solution idéale pour les entreprises qui ne veulent laisser aucune chance aux menaces APT.

McAfee® Application Control assure une sécurité sans faille en aidant l'équipe informatique à contrer les cybercriminels tout en préservant sa productivité. Grâce à son modèle d'approbation dynamique, à des informations locales et mondiales sur la réputation, à l'analyse du comportement en temps réel et à l'autoimmunisation des terminaux, cette solution McAfee neutralise instantanément les menaces APT, sans nécessiter de mises à jour des signatures ni de gestion laborieuse de listes.

Le logiciel McAfee® Change Control bloque les tentatives de modification non autorisées au niveau des configurations, des répertoires et des fichiers système critiques, tout en rationalisant la mise en œuvre des nouvelles stratégies et mesures de conformité. Grâce à ses fonctions de contrôle de l'intégrité des fichiers et de blocage des modifications, McAfee Change Control met en œuvre les stratégies de modification et assure une surveillance continue des systèmes critiques.

Il détecte et bloque en outre les modifications indésirables apportées aux systèmes sur les sites distants et distribués. Son interface de recherche intuitive permet aux utilisateurs de cibler rapidement les informations relatives aux événements de modification.

La solution combinée McAfee Application and Change Control garantit l'intégrité des systèmes en soumettant l'accès aux équipements à une autorisation explicite et en bloquant les exécutables non autorisés. Elle permet en outre de surveiller et d'empêcher les modifications apportées au système de fichiers, au Registre et aux comptes d'utilisateur en adoptant une approche systématique. Vous bénéficiez ainsi en continu d'une détection et d'une protection performantes à l'échelle de l'entreprise.

Technologie de liste blanche intelligente

Prévenez les attaques « jour zéro » et APT en bloquant les applications non autorisées et en autorisant uniquement l'exécution des applications fiables connues.

Principaux avantages

- Services de réputation des fichiers et des applications au niveau mondial et local grâce à McAfee Global Threat Intelligence et à McAfee Threat Intelligence Exchange
- Renforcement de la sécurité et réduction des coûts de possession au moyen d'une technologie de liste blanche dynamique qui valide automatiquement les nouveaux logiciels ajoutés via les sources de confiance définies
- Mise en œuvre des contrôles sur les serveurs, les machines virtuelles, les terminaux, les équipements fixes tels que les terminaux de point de vente, ainsi que les anciens systèmes, qu'ils soient connectés ou non

Gardez le contact

McAfee Application and Change Control regroupe les fichiers binaires (.exe, .dll, pilotes et scripts) présents au sein de l'environnement d'entreprise, par application et par éditeur, et les présente dans un format intuitif et hiérarchique. Elle les classe par ailleurs dans trois catégories : fiables connues, inconnues et malveillantes connues.

Mise en œuvre d'une sécurité taillée sur mesure

Dans un contexte où le cloud et les réseaux sociaux font partie intégrante des environnements d'entreprise, une plus grande flexibilité de l'accès aux applications est essentielle. C'est pourquoi McAfee Application and Change Control offre aux entreprises trois options (illustrées ci-dessous) pour optimiser leur stratégie de liste blanche en matière de prévention des menaces.

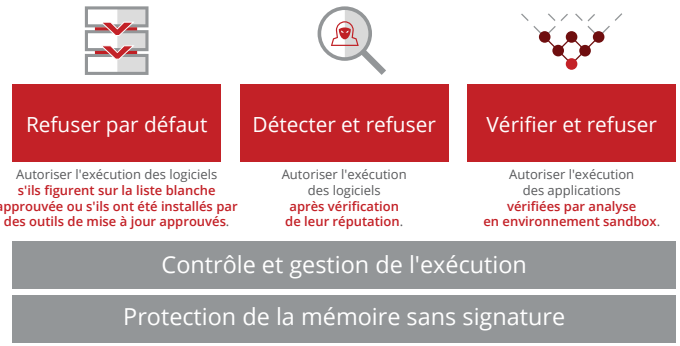

Figure 1. Trois méthodes pour optimiser la stratégie de liste blanche

Réponses rapides et exhaustives

L'ajout à la liste blanche est optimisé grâce à la cyberveille McAfee® Global Threat Intelligence, une technologie exclusive de McAfee qui contrôle en temps réel la réputation des fichiers, des messages et de leurs expéditeurs à l'aide de millions de sondes implantées aux quatre coins du monde. McAfee Application Control s'appuie sur ces connaissances pour déterminer la réputation des fichiers présents dans l'environnement informatique et les classer en tant que fichiers légitimes, malveillants ou inconnus.

Lorsqu'il est déployé en combinaison avec McAfee® Threat Intelligence Exchange, un module en option vendu séparément, McAfee Application and Change Control met à jour la liste blanche en fonction des informations locales sur la réputation afin de neutraliser instantanément les menaces. Il utilise également McAfee Threat Intelligence Exchange pour se coordonner avec McAfee® Advanced Threat Defense afin d'analyser dynamiquement le comportement des applications inconnues en environnement sandbox et de protéger automatiquement les terminaux contre les nouveaux logiciels malveillants identifiés.

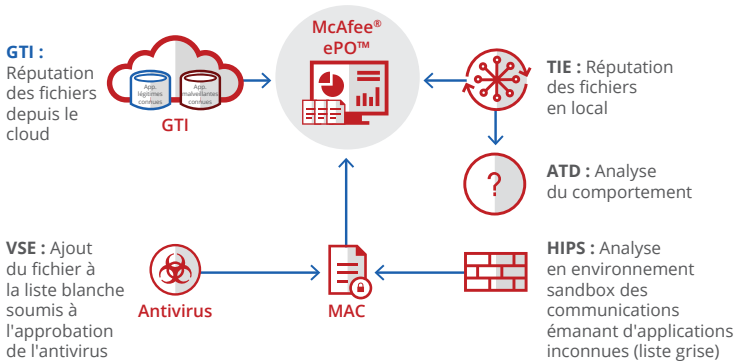

Figure 2. McAfee Global Threat Intelligence et McAfee Threat Intelligence Exchange fournissent en outre des services de réputation des fichiers et des applications au niveau mondial et local pour McAfee Application Control.

Principaux avantages (suite)

- Autorisation de nouvelles applications en fonction de leur réputation ou par une fonction d'autoapprobation pour une continuité des activités renforcée
- Visibilité ininterrompue et gestion en temps réel des modifications des fichiers système, de contenu et de configuration critiques
- Blocage des modifications des clés de Registre et des fichiers critiques par des tiers non autorisés
- Mise en œuvre stricte des stratégies grâce au blocage proactif des modifications hors processus et indésirables avant leur application

Interface de suggestions intégrée et puissante

La recherche dans l'inventaire et les rapports prédéfinis permettent aux utilisateurs de gérer facilement les problèmes de vulnérabilité, de conformité et de sécurité au sein des environnements et des fichiers liés aux applications. Ils fournissent des informations utiles, notamment sur les applications ajoutées récemment, les fichiers binaires non certifiés, les fichiers à la réputation inconnue et les systèmes exécutant des versions logicielles obsolètes.

Par ailleurs, le nouveau mode Inventaire de McAfee Application and Change Control 8.3 maintient en permanence à jour les inventaires de chaque système/équipement. Cela permet de réduire l'utilisation des ressources du processeur et du système/de l'équipement tout en maintenant la conformité aux normes SWAM/CPE et PCI-DSS. Le mode Inventaire permet aux utilisateurs de suivre les modifications apportées au fil du temps aux fichiers et fichiers binaires présents sur le terminal. La norme CPE (Common Platform Enumeration) offre la possibilité d'associer les données CPE du NIST aux inventaires collectés pour la création de listes blanches et la génération de rapports de conformité.

Impact nul sur la continuité des activités

Pour éviter toute interruption des opérations, les nouvelles applications sont automatiquement autorisées ou non à s'exécuter en fonction de leur réputation. Lorsque ces applications sont inconnues, une interface de suggestions recommande de nouvelles stratégies de mise à jour fondées sur les comportements d'exécution au niveau des terminaux. Cette approche permet une gestion optimale des exceptions générées par les applications bloquées. En effet, après avoir inspecté ces exceptions et les informations sur l'application, il suffit soit d'autoriser cette dernière en ajoutant son fichier à la liste blanche, soit de l'ignorer pour la bloquer.

Participation active des utilisateurs

Pour les applications inconnues, McAfee Application and Change Control explique aux utilisateurs pourquoi l'accès aux applications non autorisées est bloqué et leur permet de prendre des mesures pour les faire approuver par le biais d'auto-approbations ou de demandes d'approbation.

Maintien des systèmes à jour

La tenue à jour de systèmes par l'installation des derniers patchs disponibles est essentielle. Le modèle d'approbation dynamique de McAfee Application and Change Control permet l'actualisation automatique des systèmes sans affecter la continuité des activités. Il permet d'utiliser des sources approuvées pour les mises à jour : utilisateurs, groupes locaux, certificats, processus ou encore répertoires. McAfee Application Control empêche également les applications sur liste blanche d'être exploitées dans le cadre d'attaques par débordement de mémoire tampon sur les systèmes Microsoft Windows.

Prévention des modifications et contrôle de l'intégrité

Les risques d'écarts de configuration et le manque de visibilité sur les auteurs des modifications peuvent entraîner des compromissions de sécurité, des fuites de données ou des pannes. McAfee Application and Change Control permet de bloquer ou de restreindre toute tentative de modification non conforme aux stratégies définies effectuée sur le système/l'équipement.

Plates-formes prises en charge

McAfee Application and Change Control :

- Versions 8.3.x, 8.2.x, 8.1.x, 8.0.x et 7.0.x (systèmes d'exploitation Windows)
- Versions 6.4.x et 6.3.x (systèmes d'exploitation Linux) et versions 6.2.x et 6.1.x (systèmes d'exploitation Windows et de type UNIX)
- Linux
- Microsoft Windows

Chaque tentative de modification est enregistrée afin d'assurer la visibilité en temps réel sur les événements de modification. Le module du contrôleur système gère les communications entre le contrôleur système et les agents.

Contrôle de l'intégrité des fichiers de nouvelle génération

McAfee Application and Change Control permet l'implémentation d'un logiciel de contrôle de l'intégrité des fichiers en temps réel et la validation de la conformité PCI-DSS de manière efficace et rentable. Le module de contrôle de l'intégrité des fichiers de McAfee Application and Change Control répond aux questions essentielles (qui, quand, quoi et pourquoi) en indiquant l'utilisateur, l'heure de la modification, le nom du programme et les données des fichiers ou du Registre concernés, en un seul endroit et en temps réel. Il permet en outre d'identifier les causes fondamentales d'une interruption de service lors d'une opération de dépannage.

Suivi des modifications du contenu

McAfee Change Control permet à l'équipe informatique de suivre les modifications du contenu et des attributs de fichiers. Les modifications du contenu des fichiers peuvent être affichées et comparées côte à côte afin d'identifier les ajouts, suppressions et modifications effectués. Des filtres d'inclusion et d'exclusion peuvent être configurés de façon à ce que seules les modifications pertinentes et exploitables soient enregistrées. Les modifications des systèmes et des équipements peuvent également être limitées en fonction des utilisateurs, groupes d'utilisateurs locaux, applications, certificats et/ou services web.

Elles peuvent même être limitées à des heures et des dates précises (par exemple, l'application des mises à jour de Windows peut être autorisée uniquement entre 2h et 4h du matin le mardi). Par ailleurs, des mécanismes d'alerte spéciaux informent immédiatement l'équipe informatique des modifications critiques afin d'éviter les interruptions liées à la configuration — une des meilleures pratiques recommandées par ITIL (Information Technology Infrastructure Library). Des formulaires QSA (Évaluateur qualifié en matière de sécurité) sont également fournis pour simplifier la génération de rapports PCI.

Prévention des interruptions liées à des modifications non planifiées

McAfee Change Control permet à l'équipe informatique de résoudre facilement les incidents, d'automatiser les contrôles de conformité réglementaire et de prévenir les interruptions liées aux modifications. Il n'est plus nécessaire de recourir à des stratégies de conformité manuelles, propices aux erreurs et sollicitant d'importantes ressources, qui sont souvent associées à la loi Sarbanes-Oxley, par exemple. McAfee Application and Change Control permet aux utilisateurs de créer un cadre automatisé de contrôles informatiques où toutes les informations nécessaires pour vérifier la conformité sont contenues dans un système unique de génération de rapports. Les modifications contraires aux autorisations peuvent être validées automatiquement. Les correctifs d'urgence et autres modifications hors processus sont automatiquement documentés et rapprochés pour faciliter les audits.

Gestion centralisée de la sécurité et de la conformité

Le logiciel McAfee® ePolicy Orchestrator® (McAfee ePO™) consolide et centralise la gestion, offrant ainsi une vue globale sur la sécurité de l'entreprise. Cette plate-forme primée intègre McAfee Application and Change Control avec McAfee® Host Intrusion Prevention et d'autres produits de sécurité McAfee, notamment des produits de protection antimalware pour offrir une fonctionnalité de liste noire. McAfee Application and Change Control peut en outre être installé et mis à jour en une seule étape depuis Microsoft System Center. De nouveaux profils peuvent être activés à tout moment pour renforcer la protection, d'une simple surveillance à une mise en œuvre hypersécurisée.

Étapes suivantes

Empêchez efficacement les applications non autorisées de s'exécuter d'une manière susceptible de mettre les données en péril, et adoptez une approche systématique du contrôle et de la prévention des modifications du système de fichiers, du Registre et des comptes d'utilisateurs. McAfee Application and Change Control garantit l'intégrité des systèmes en soumettant l'accès aux équipements à une autorisation explicite et en bloquant les exécutables non autorisés.

Pour plus d'informations, consultez notre site à l'adresse www.mcafee.com/fr/products/application-control.aspx ou appelez le +33 1 47 62 56 00 (standard) — numéro accessible aux heures de bureau.

En savoir plus

Pour plus d'informations, consultez notre guide des environnements pris en charge (KB87944).

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr