McAfee Application Control

Limitation des risques associés aux applications non autorisées et contrôle des terminaux, des serveurs et des équipements fixes

Face à des menaces APT exécutées par attaque à distance ou ingénierie sociale, il est de plus en plus difficile de protéger votre entreprise. McAfee® Application Control lui assure une sécurité sans faille en vous aidant à contrer les cybercriminels tout en préservant sa productivité. Grâce à son modèle d'approbation dynamique et à ses fonctionnalités de sécurité innovantes, notamment des informations locales et mondiales sur la réputation, l'analyse du comportement en temps réel et l'autoimmunisation des terminaux, cette solution de McAfee neutralise instantanément les menaces APT, sans nécessiter de mises à jour des signatures ou une gestion de listes laborieuse. McAfee Application Control est la solution idéale pour vous protéger contre les attaques « jour zéro ».

Technologie de liste blanche intelligente

McAfee Application Control prévient les attaques « jour zéro » et celles associées aux menaces APT en bloquant l'exécution des applications non autorisées. Notre fonctionnalité d'inventaire permet d'identifier et de gérer facilement les fichiers liés aux applications. Elle 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. La liste blanche intègre alors les applications fiables connues de sorte qu'elles seules sont autorisées à s'exécuter, tandis que les logiciels malveillants inconnus sont bloqués.

Mise en œuvre d'une sécurité taillée sur mesure

Dans un contexte où le cloud et les médias sociaux font partie intégrante de leurs environnements d'entreprise, les utilisateurs veulent plus de flexibilité pour pouvoir tirer parti de nouvelles applications. McAfee Application Control offre aux entreprises trois options (illustrées ci-dessous) pour optimiser leur stratégie de liste blanche en matière de prévention des menaces.

Principaux avantages

- Protection contre les attaques « jour zéro » et les menaces APT sans nécessiter de mises à jour de signatures
- 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
- Contrôle efficace de l'accès aux applications grâce à McAfee® ePolicy Orchestrator® (McAfee ePO™), plate-forme de gestion centralisée des solutions de sécurité McAfee
- Réduction des cycles d'application de patchs grâce à une liste blanche sécurisée et à la protection avancée de la mémoire
- Maintien à jour des systèmes par l'application des patchs les plus récents à l'aide d'outils de mise à jour approuvés

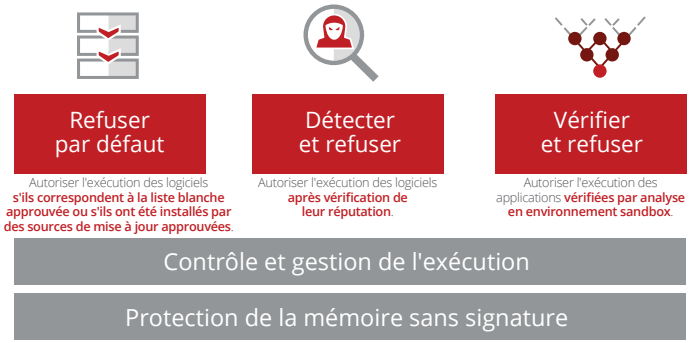

Figure 1. Trois modes pour optimiser votre stratégie de liste blanche

Interface de suggestions intégrée et puissante

Grâce à la recherche dans l'inventaire et aux rapports prédéfinis, vous pouvez détecter et résoudre rapidement les problèmes de vulnérabilités, de conformité et de sécurité au sein de votre environnement. Vous disposez d'informations utiles, concernant notamment les applications ajoutées récemment, les fichiers binaires non certifiés, les fichiers à la réputation inconnue, les systèmes exécutant des versions logicielles obsolètes, etc. Vous pouvez ainsi identifier rapidement les vulnérabilités et valider la conformité de l'entreprise en matière de licences logicielles.

Réponses rapides et exhaustives

L'ajout à la liste blanche est optimisé grâce à la cyberveille mondiale sur les menaces de McAfee Global Threat Intelligence (McAfee GTI), 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 votre environnement informatique et les classer en tant que fichiers légitimes, malveillants ou inconnus.

Lorsqu'il est déployé avec McAfee Threat Intelligence Exchange, un module en option vendu séparément, McAfee Application Control met à jour la liste blanche en fonction des informations locales sur la réputation afin de neutraliser instantanément les menaces. Grâce à McAfee Threat Intelligence Exchange, McAfee Application Control peut également collaborer avec McAfee Advanced Threat Defense pour analyser de manière dynamique le comportement des applications inconnues dans un environnement sandbox et immuniser automatiquement les terminaux contre les nouveaux logiciels malveillants détectés.

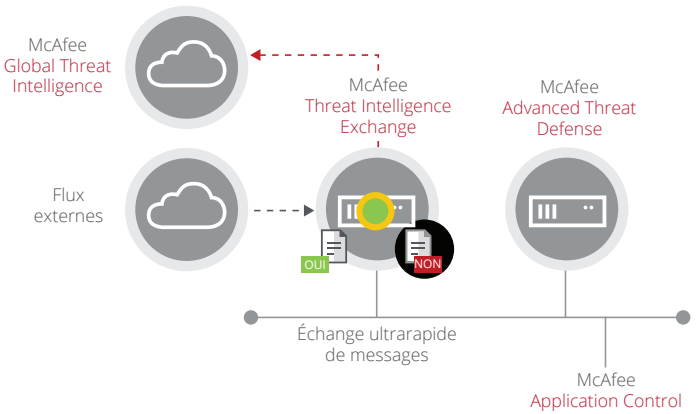

Figure 2. McAfee GTI surveille en continu la réputation des fichiers et des expéditeurs. Lorsqu'il est déployé avec McAfee Threat Intelligence Exchange, McAfee Application Control met automatiquement à jour sa liste blanche sur la base d'informations locales sur les menaces. De plus, il peut agir en coordination avec McAfee Advanced Threat Defense si d'autres informations au sujet d'un fichier se révèlent nécessaires.

Principaux avantages (suite)

- Mise en œuvre des contrôles sur les serveurs, les machines virtuelles, les terminaux, les équipements à fonction fixe (tels que les terminaux de point de vente) et les systèmes anciens (tels que Microsoft Windows XP), qu'ils soient connectés ou non
- Autorisation de nouvelles applications en fonction de leur réputation ou par une fonction d'autoapprobation pour une continuité des activités améliorée
- Maintien de la productivité des utilisateurs et des performances du serveur grâce à cette solution peu gourmande en ressources
- Protection aisée des systèmes anciens et des investissements dans les technologies modernes

Plates-formes prises en charge

Microsoft Windows (32 et 64 bits)

- Systèmes embarqués : Windows XPE, 7 Embedded, WEPOS, POSReady 2009, WES 2009, Embedded 8, 8.1 Industry et 10
- Serveurs : Windows Server 2008, 2008 R2, 2012 et 2012 R2
- Postes de travail : Windows NT, 2000, XP, Vista, 7, 8, 8.1 et 10

Linux

- Red Hat/CentOS 5, 6 et 7
- SUSE/openSUSE 10 et 11
- Oracle Enterprise Linux 5, 6 et 7
- Ubuntu 12.04

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

McAfee Application Control offre à l'équipe informatique de nombreuses méthodes permettant aux utilisateurs d'installer de nouvelles applications inconnues :

- **Notifications utilisateur** — Les utilisateurs peuvent recevoir des messages pop-up leur expliquant la raison du refus d'accès aux applications non autorisées. Ces messages les invitent à solliciter l'approbation de l'application par e-mail ou auprès d'un centre d'assistance.
- **Autoapprobations des utilisateurs** — Les utilisateurs détenteurs de ce privilège ne sont pas obligés d'attendre l'approbation du département informatique pour installer de nouveaux logiciels. Le responsable informatique peut inspecter ces autoapprobations et créer des stratégies à l'échelle de l'entreprise pour interdire ou autoriser l'application sur l'ensemble des systèmes.

Maintien à jour de vos systèmes

Nous sommes conscients de l'importance que revêt la tenue à jour de vos systèmes par l'installation des derniers patchs disponibles. C'est d'ailleurs la raison pour laquelle nous proposons un modèle d'approbation dynamique permettant l'actualisation de vos systèmes sans affecter la continuité des activités. Ce modèle vous permet d'utiliser des sources approuvées pour les mises à jour : utilisateurs, 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 32 et 64 bits.

Contrôle avancé de l'exécution

McAfee Application Control permet de combiner des règles basées sur le nom du fichier, le nom du processus, le nom du processus parent, les paramètres de ligne de commande et le nom de l'utilisateur afin d'offrir une protection renforcée. Vous pouvez utiliser le contrôle avancé de l'exécution pour stopper les attaques qui contournent les entrées-sorties de fichier, bloquer le mode interactif pour les interpréteurs système et empêcher l'exploitation par les outils système. Vous pouvez en outre créer des stratégies fondées sur l'algorithme SHA-256, plus puissant et robuste.

McAfee ePolicy Orchestrator, pour une gestion efficace et centralisée

Le logiciel McAfee ePO offre les avantages d'une gestion consolidée et centralisée : il propose une vue globale, sans « angles morts », sur la sécurité de votre entreprise. Cette plate-forme primée intègre McAfee Application 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 Control peut en outre être installé et mis à jour en une seule étape depuis Microsoft System Center.

Un mode d'observation pour optimiser votre utilisation

Le mode d'observation vous offre la possibilité de découvrir des stratégies destinées aux environnements de postes de travail dynamiques sans verrouiller la liste blanche. Il vous permet de déployer progressivement McAfee Application Control dans des environnements de préproduction ou de début de production sans perturber le fonctionnement des applications. Avec McAfee Application Control, les administrateurs peuvent utiliser une page de découverte des stratégies unique pour définir des stratégies pour les observations et les demandes d'autoapprobation.

Protection des systèmes anciens et des investissements en nouvelles technologies

Vous souhaitez protéger des systèmes d'exploitation plus anciens, tels que Microsoft Windows NT, Windows 2000 et Windows XP ? Bien que de tels systèmes ne soient pas pris en charge par Microsoft et d'autres éditeurs de solutions de sécurité, vous n'avez aucun souci à vous faire grâce à McAfee Application Control. Qui plus est, la solution prend en charge les systèmes d'exploitation récents, notamment Microsoft Windows 10.

Étapes suivantes

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.

McAfee
Together is power.

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