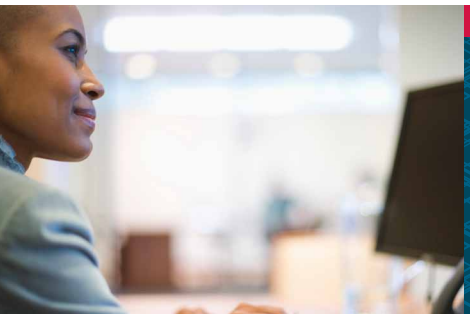

L'évolution du paysage de la sécurité des postes de travail

Le paysage de la sécurité des postes de travail a évolué sous l'influence de plusieurs facteurs, notamment les logiciels malveillants (***malware***) ciblés, les préoccupations liées au confort de l'utilisateur final ou encore les coûts des opérations et de support informatique. En règle générale, la mise en œuvre d'une solution de sécurisation des postes de travail peut être comparée à la souscription d'une police d'assurance contre des risques potentiels qui ne tient pas véritablement compte des autres facteurs. Dans l'environnement d'exploitation courant (COE, *Common Operating Environment*) de l'entreprise, la sécurisation des postes de travail est devenue un véritable casse-tête pour les équipes informatiques forcées de trouver le juste compromis entre flexibilité pour l'utilisateur final et exigences en termes de sécurité.

Environnements de postes de travail

Comme le suggèrent diverses études, il existe deux catégories d'environnements de postes de travail :

- *Utilisateurs standard* — Leurs postes de travail utilisent des images COE figées. Ils sont également appelés postes de travail à fonction fixe ou à image commune. Dans ce type d'environnement, l'utilisateur final ne dispose pas des privilèges nécessaires pour installer ou désinstaller des logiciels. *Exemples :* postes de travail des secteurs du commerce de détail, financier et hospitalier.
- *Utilisateurs avec privilèges* — Ces utilisateurs sont autorisés à installer les logiciels de leur choix. *Exemples :* environnements d'ingénierie et de conception graphique.

Dans le cadre de ce document, nous nous concentrerons sur le modèle de sécurité de l'environnement COE.

Les défis actuels de la sécurité des postes de travail

Avec l'avènement progressif de l'économie de la connaissance ces vingt dernières années, les défis liés au maintien de l'inaltérabilité de l'infrastructure informatique se sont considérablement compliqués. Les chercheurs du monde entier ont constaté une hausse massive du nombre d'échantillons de logiciels malveillants, de quelques milliers en une année à l'époque à quelques milliers par jour aujourd'hui. Sur le plan opérationnel, la protection des postes clients (postes de travail et ordinateurs portables) a gagné en complexité, et de fait, bien souvent, les problèmes signalés par les responsables de la sécurité informatique sont liés aussi bien à la sécurité opérationnelle qu'aux menaces.

Prolifération des logiciels malveillants

Premièrement, la multiplication phénoménale des logiciels malveillants en circulation constitue la préoccupation majeure des responsables de la sécurité. On constate un net accroissement tant de la complexité que du nombre de logiciels malveillants qui fournissent plusieurs vecteurs d'attaques contre les infrastructures informatiques.

Performances

Deuxièmement, les performances des solutions traditionnelles demeurent une source d'inquiétudes, notamment en raison de la hausse considérable du nombre de signatures de logiciels malveillants.

Sécurité des opérations

Troisièmement, l'aspect opérationnel de la sécurité pose un problème majeur. Lorsque des logiciels malveillants transitent par un environnement informatique, ils rendent déficiente l'infrastructure de sécurité. En outre, les solutions de sécurité traditionnelles, basées sur les signatures, risquent de ne pas être à même de réduire l'exposition aux attaques de type « jour zéro » et aux menaces persistantes avancées.

Multiplication des applications non autorisées

Enfin, la prolifération des applications non autorisées sur les postes de travail des utilisateurs doit impérativement être maîtrisée. Dans les marchés émergents, cela implique également d'empêcher les logiciels piratés et dépourvus de licences de se répandre dans l'environnement d'entreprise.

Difficultés comportementales de la gestion de la sécurité

Sur le plan du comportement, les environnements COE sont le théâtre d'une lutte incessante entre la nécessité pour l'administrateur de mettre en œuvre la sécurité et le besoin pour l'utilisateur final de disposer d'un environnement sécurisé mais néanmoins flexible. Ces deux objectifs doivent être atteints, sans toutefois sacrifier la sécurité ou la productivité dans l'entreprise. La solution adoptée doit, pour ce faire, satisfaire les exigences de sécurité de l'administrateur et de l'utilisateur, sans compromettre le principe primordial de productivité durable.

Comment résoudre ces problèmes ?

Grâce à ses fonctions de listes d'autorisation, McAfee® Application Control, allié à la technologie antivirus traditionnelle, offre une solution efficace à bon nombre de ces problèmes. Grâce à sa grande résistance aux logiciels malveillants et à ses fonctions améliorées de gestion des attaques, McAfee Application Control constitue une nette amélioration par rapport aux solutions classiques de sécurisation des postes de travail.

Listes d'autorisation d'applications

L'approche des listes d'autorisation est essentiellement fondée sur l'identification des fichiers légitimes connus d'un environnement informatique, qui permet d'autoriser uniquement les fichiers légitimes connus sur le système. Elle peut être mise en œuvre de différentes façons : soit via un déploiement autonome de la solution de listes d'autorisation, soit par sa combinaison avec une solution de listes de blocage traditionnelle, telle qu'un antivirus. L'environnement informatique envisagé ici utilise un logiciel antivirus qui peut être optimisé par l'intégration d'une technologie de listes d'autorisation.

Mode d'observation

McAfee Application Control propose un mode de fonctionnement nommé « mode d'observation ». Il n'y a pas de mise en œuvre dans ce mode puisqu'il ne fait que surveiller les versions de McAfee Application Control. Il peut être activé lorsque McAfee Application Control a été installé et a effectué une analyse de l'inventaire. Dans le cadre du déploiement initial au sein d'une entreprise, ce mode peut faciliter l'élaboration de stratégies qui aident à détecter toute non-conformité aux règles de sécurité et identifie les exceptions opérationnelles valides.

Lors d'un déploiement de la solution avec un outil antivirus conventionnel, le mode d'observation permet à l'antivirus de continuer à fonctionner en tant qu'outil de sécurité principal. L'administrateur de la sécurité peut ainsi surveiller les actifs informatiques, tout en laissant à l'antivirus le soin de gérer la sécurité au niveau des postes clients des utilisateurs. D'une manière générale, cette approche permet à l'utilisateur d'être plus productif, et à l'administrateur informatique, de bénéficier d'informations sur la sécurité plus pertinentes.

Evaluation de la réputation des fichiers grâce à McAfee Global Threat Intelligence™ (McAfee GTI™)

McAfee Application Control comprend également des fonctions d'évaluation de la réputation des fichiers basées sur McAfee GTI. Cette intégration lui permet d'extraire l'inventaire de fichiers complet des postes clients pour ensuite le diffuser à McAfee® ePolicy Orchestrator® (McAfee ePO™). L'inventaire est ensuite comparé aux scores de réputation des fichiers reçus du serveur McAfee GTI. Cette analyse, effectuée hors ligne et avec un transfert de la charge, permet de vérifier si des fichiers de l'entreprise constituent des logiciels malveillants ou sont autrement indésirables. S'il est établi que le fichier est un logiciel malveillant, l'interface McAfee ePO offre la possibilité, via sa console de gestion centralisée, de rechercher rapidement l'emplacement de toutes les instances de la menace dans l'ensemble de l'environnement.

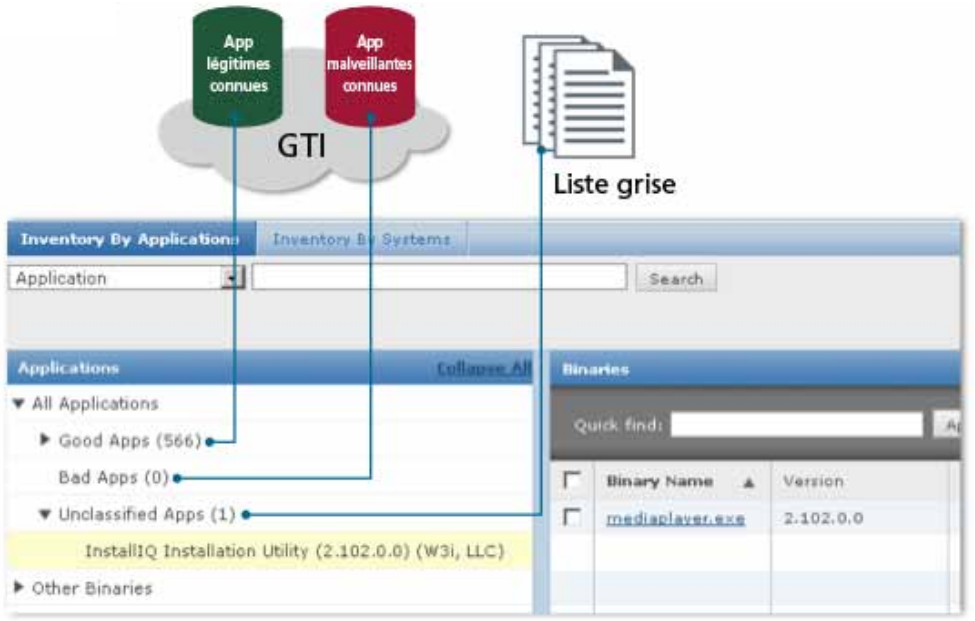

Figure 1. Le service de réputation de fichiers McAfee GTI classe par catégorie toutes les applications de l'entreprise.

Résistance aux attaques de logiciels malveillants

La possibilité d'exécuter McAfee Application Control en mode d'observation — l'antivirus tenant le rôle de logiciel de sécurité principal — offre un avantage inégalé en termes de résistance aux attaques de logiciels malveillants, en plus de permettre à l'administrateur de passer du mode d'observation au mode de mise en œuvre et inversement lorsque les circonstances l'exigent. Dès lors qu'une attaque de logiciel malveillant est suspectée, le passage de McAfee Application Control en mode de mise en œuvre fige l'état du système dans l'ensemble de l'infrastructure informatique, et empêche par conséquent le logiciel malveillant de s'infiltrer plus avant dans l'entreprise. Grâce à cette approche et à la possibilité de gérer la détection des logiciels malveillants basée sur l'inventaire dans le logiciel McAfee ePO, la correction des systèmes infectés s'effectue de façon plus simple et rapide.

Interaction des utilisateurs avec les listes d'autorisation dynamiques

Si McAfee Application Control est déployé en mode de mise en œuvre et s'exécute par conséquent à un niveau de sécurité supérieur, l'utilisateur final qui souhaite apporter des modifications à son ordinateur doit en faire la demande auprès de l'équipe informatique afin que celle-ci donne son approbation. Ce processus constitue la partie dynamique des listes d'autorisation, qui passe par une interaction bien définie entre l'utilisateur et l'administrateur. Grâce à cette fonctionnalité, McAfee Application Control est capable d'offrir une sécurité accrue, tout en gérant l'expérience utilisateur à un niveau identique à celui d'un outil antivirus traditionnel.

Figure 2. Notifications affichées sur le poste de travail et demande d'approbation d'applications ne figurant pas dans la liste d'autorisation.

Gestion des applications autorisées

Dans les marchés émergents, le contexte de sécurité se définit également par la possibilité de détecter les logiciels non sécurisés et non autorisés dans un environnement informatique. Etant donné que l'inventaire est disponible dans le logiciel McAfee ePO, il est possible de l'exporter et de le rapprocher avec une liste des logiciels sécurisés et approuvés par l'entreprise. Les divergences entre cette liste et l'inventaire exporté par McAfee ePO peuvent être utilisées pour identifier les infractions aux stratégies de sécurité générales et aux exigences en matière de licences, le cas échéant.

Conclusion

Les listes d'autorisation d'applications constituent désormais une couche de sécurité essentielle et efficace pour une certaine catégorie de postes de travail. Conjuguées aux solutions antivirus actuelles, elles offrent non seulement une protection robuste contre les menaces émergentes, telles que les menaces persistantes avancées et les logiciels malveillants ciblés, mais elles contribuent également à réduire les coûts opérationnels en maîtrisant la prolifération des applications non autorisées. Grâce aux nombreux avantages de ces listes et aux récents progrès technologiques facilitant la mise en œuvre des listes d'autorisation en général, les administrateurs peuvent espérer un modèle de sécurisation des postes de travail plus simple.

A propos de McAfee

McAfee, filiale à part entière d'Intel Corporation (NASDAQ : INTC), est la plus grande entreprise au monde entièrement dédiée à la sécurité informatique. Elle propose dans le monde entier des solutions et des services proactifs et réputés, qui assurent la sécurisation des systèmes, des réseaux et des équipements mobiles et qui permettent aux utilisateurs de se connecter à Internet, de surfer ou d'effectuer leurs achats en ligne en toute sécurité. Grâce au soutien de son système hors pair de renseignement sur les menaces, Global Threat Intelligence, McAfee crée des produits innovants au service des particuliers, des entreprises, du secteur public et des fournisseurs de services, pour les aider à se conformer aux réglementations, à protéger leurs données, à prévenir les perturbations dans le flux des activités, à identifier les vulnérabilités ainsi qu'à surveiller et à améliorer en continu leurs défenses. McAfee consacre tous ses efforts à trouver des solutions novatrices afin d'assurer à ses clients une protection irréprochable. www.mcafee.com/fr

McAfee
An Intel Company

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr

41101brf_desktop-security_0112_fnl_ETMG