McAfee Embedded Control

Intégrité du système, contrôle des modifications et conformité aux stratégies dans une solution unique

McAfee® Embedded Control préserve l'intégrité de votre système en autorisant uniquement l'exécution de code approuvé et l'implémentation des modifications autorisées. Il crée automatiquement une liste blanche dynamique de « code autorisé » sur le système embarqué. Une fois cette liste blanche créée et activée, le système est verrouillé avec la ligne de base correcte connue. Aucun programme ou code hormis ceux qui ont été approuvés ne peut s'exécuter et aucune modification non autorisée ne peut être effectuée. McAfee Integrity Control, qui associe McAfee Embedded Control et la console McAfee ePolicy Orchestrator® (McAfee ePO™), propose des rapports d'audit et de conformité intégrés qui vous aident à respecter les diverses réglementations de conformité applicables.

McAfee Embedded Control a été conçu pour résoudre le risque de sécurité accru posé par l'adoption de systèmes d'exploitation commerciaux dans les systèmes embarqués. Cette solution de sécurité indépendante des applications, peu encombrante et peu gourmande en ressources, est simple à déployer et ne nécessite aucune intervention ultérieure. McAfee Embedded Control convertit un système exécutant un système d'exploitation commercial en une « boîte noire » pour en faire un système d'exploitation propriétaire fermé. Il empêche ainsi tout programme non autorisé résidant sur disque ou injecté dans la mémoire de s'exécuter et d'apporter des modifications non autorisées à une ligne de base approuvée. Cette solution permet aux fabricants de profiter de tous les avantages d'un système d'exploitation commercial sans courir de risque supplémentaire ni perdre le contrôle de son utilisation après sa mise en service.

Intégrité du système garantie

Contrôle des fichiers exécutables

Avec McAfee Embedded Control, seuls les programmes figurant dans la liste blanche dynamique McAfee peuvent être exécutés. Les autres programmes, dont les fichiers exécutables, les bibliothèques de liaisons dynamiques (DLL) et les scripts, sont considérés comme non autorisés. Leur exécution est bloquée et ce blocage est consigné par défaut. De cette façon, les vers, les virus, les logiciels espions (spyware) et autres logiciels malveillants (malware) qui tentent de s'installer ne parviennent pas à s'exécuter.

Principaux avantages

- Limitation des risques de sécurité grâce au contrôle du code et des applications exécutés sur vos équipements embarqués et à la protection de la mémoire de ces équipements
- Gestion de l'accès, maintien du contrôle et diminution des coûts du support technique
- Mise en œuvre sélective
- Déploiement simple, sans intervention ultérieure
- Préparation de l'audit et de la mise en conformité des équipements
- Visibilité en temps réel
- Audit complet
- Archive des modifications indexée
- Rapprochement en boucle fermée

Contrôle de la mémoire

Le contrôle de la mémoire permet de protéger les processus en cours d'exécution contre les tentatives de piratage. Le code non autorisé injecté dans un processus en exécution est intercepté, bloqué et consigné. Il est ainsi possible de neutraliser et de journaliser toute tentative de prise de contrôle d'un système par divers exploits, dont les exploits par débordement de mémoire tampon, du tas et de la pile[1].

Intégration de McAfee GTI : pour une gestion optimale des menaces au niveau mondial dans les environnements isolés

McAfee Global Threat Intelligence (McAfee GTI) est une technologie exclusive de McAfee qui contrôle la réputation des fichiers, des messages et de leurs expéditeurs en temps réel à l'aide de millions de sondes implantées aux quatre coins du monde. Elle s'appuie sur des connaissances tirées du cloud pour déterminer la réputation de tous les fichiers présents dans votre environnement informatique et les classer en tant que fichiers légitimes, malveillants ou inconnus. Grâce à l'intégration de McAfee GTI, plus aucune inscription malencontreuse d'un fichier malveillant dans les listes blanches ne passera inaperçue. Les services de réputation GTI sont accessibles à partir des environnements logiciels McAfee ePO connectés à Internet ou isolés.

Contrôle des modifications

McAfee Embedded Control détecte les modifications en temps réel. Il procure une excellente visibilité sur les sources de modification et vérifie que les modifications ont été déployées sur les systèmes cibles corrects. Il fournit une piste d'audit des modifications et fait en sorte que seules les sources approuvées puissent apporter des modifications.

McAfee Embedded Control permet de mettre en œuvre des processus de contrôle des modifications en spécifiant les modalités de modification autorisées. Vous pouvez ainsi spécifier les utilisateurs autorisés à effectuer des modifications, les certificats requis pour autoriser les modifications, les éléments qui peuvent être modifiés (par exemple, certains fichiers ou répertoires uniquement) ainsi que les périodes autorisées (en limitant par exemple les mises à jour de Microsoft Windows à certaines périodes de la semaine).

Un module de validation des modifications proactif permet de vérifier chaque modification avant son application sur les systèmes cibles. Lorsque ce module est activé, les mises à jour de logiciels doivent respecter un processus de contrôle déterminé.

Le module de suivi des modifications en temps réel consigne toutes les modifications apportées à l'état du système, notamment au code, à la configuration et au Registre. Les événements de modification sont journalisés au moment où ils se produisent et envoyés au contrôleur système à des fins d'agrégation et d'archivage.

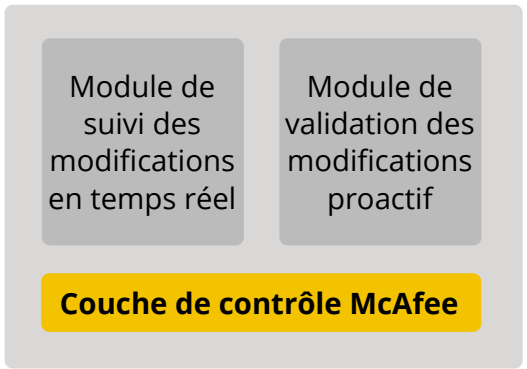

Figure 1. Couche de contrôle McAfee

Le module du contrôleur système gère les communications entre le contrôleur système et les agents. Il agrège et enregistre les informations concernant les événements de modification envoyés par les agents au système d'enregistrement indépendant.

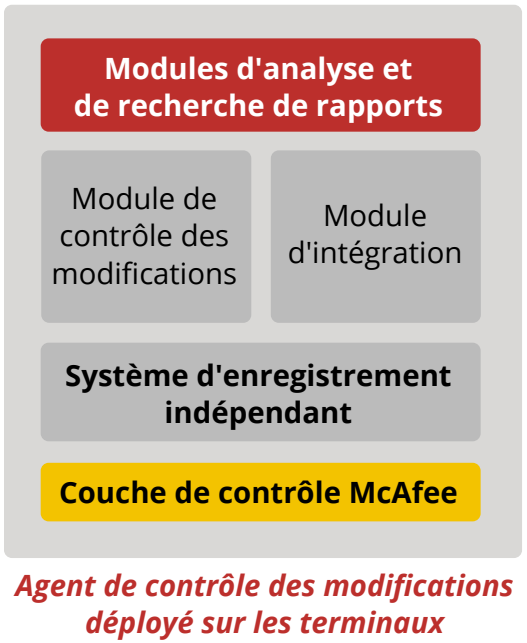

Figure 2. Modules d'analyse, de recherche et de génération de rapports

Audit et conformité aux stratégies

McAfee Integrity Control fournit des tableaux de bord et des rapports qui vous aident à respecter vos impératifs de conformité. Ils sont générés via la console McAfee ePO, qui offre une interface utilisateur web aux utilisateurs et aux administrateurs.

McAfee Embedded Control propose des fonctions d'audit et de conformité en temps réel, intégrées et en boucle fermée, associées à un système d'enregistrement des activités autorisées et des tentatives non autorisées qu'il est impossible de falsifier ou de manipuler.

À propos des solutions de sécurité embarquée de McAfee

Grâce aux solutions de sécurité embarquée de McAfee, les fabricants ont l'assurance que leurs produits et équipements sont protégés contre les cybermenaces et les attaques. Ces solutions couvrent un large éventail de technologies dont les listes blanches d'applications, la protection antivirus et antimalware, la gestion des équipements, le chiffrement ainsi que la gestion des risques et de la conformité ; de plus, toutes exploitent McAfee Global Threat Intelligence, notre système mondial réputé de renseignements sur les menaces. Nos solutions peuvent être adaptées pour répondre aux exigences de conception propres à l'équipement d'un fabricant et à ses architectures.

Fonctionnalité	Description	Avantage
Intégrité du système garantie		
Protection contre les menaces externes	Garantit que seul le code autorisé peut s'exécuter. Le code non autorisé ne peut pas être injecté dans la mémoire. Le code autorisé ne peut pas être falsifié ni manipulé.	▪ Élimine l'application de patchs dans l'urgence, diminue le nombre et la fréquence des corrections, permet d'effectuer des tests plus approfondis avant la correction, réduit le risque de sécurité sur les systèmes sur lesquels il est difficile d'installer des patchs. ▪ Limite le risque de sécurité posé par des attaques polymorphes de type « jour zéro » par des logiciels malveillants tels que les vers, les virus et les chevaux de Troie ou encore les injections de code, par exemple les attaques par débordement de mémoire tampon, du tas et de la pile. ▪ Préserve l'intégrité des fichiers autorisés en vérifiant que le système de production présente un état connu et vérifié. ▪ Diminue le coût des opérations en limitant les temps d'arrêt liés à l'application de patchs et aux reprises non planifiées, tout en améliorant la disponibilité du système.
Protection contre les menaces internes	Permet un verrouillage local des administrateurs pour empêcher ceux-ci de modifier les processus autorisés à s'exécuter sur un système protégé sauf s'ils le font à l'aide d'une clé authentique.	▪ Assure une protection contre les menaces internes. ▪ Verrouille tous les éléments exécutés sur les systèmes embarqués en service et bloque les modifications, même si elles sont effectuées par des administrateurs.

Étapes suivantes

Pour plus d'informations, consultez notre site à l'adresse **www.mcafee.com/fr/partners/oem-alliances/index.aspx** ou contactez votre représentant McAfee local.

FICHE TECHNIQUE

Fonctionnalité	Description	Avantage
Contrôle des modifications avancé		
Protection des mises à jour autorisées par le fabricant	Garantit que seules les mises à jour autorisées peuvent être effectuées sur des systèmes embarqués en service.	▪ Fait en sorte qu'aucune modification hors bande ne puisse être déployée sur les systèmes en service. Bloque les modifications non autorisées du système avant qu'elles n'entraînent des interruptions de service et des appels au support technique. ▪ Permet aux fabricants soit de conserver le contrôle total des modifications, soit d'autoriser uniquement des agents approuvés du client à les contrôler.
Contrôle des modifications apportées pendant la période autorisée	Garantit qu'aucune modification n'est implémentée en dehors des périodes de modification autorisées.	▪ Bloque les modifications non autorisées pendant les périodes critiques en termes d'obligations fiscales ou les heures de pointe pour éviter toute interruption des opérations et/ou des infractions aux impératifs de conformité.
Outils ou personnel autorisés pour les mises à jour	Garantit que seuls les processus et les membres du personnel autorisés peuvent implémenter des modifications sur les systèmes de production.	▪ Fait en sorte qu'aucune modification hors bande ne puisse être déployée sur les systèmes de production.
Audit et conformité en boucle fermée et en temps réel		
Suivi des modifications en temps réel	Effectue le suivi de toutes les modifications intervenant dans l'entreprise.	▪ Fait en sorte qu'aucune modification hors bande ne puisse être déployée sur les systèmes de production.
Audit complet	Collecte des informations complètes sur chaque modification apportée au système : auteur, date et heure et emplacement de la modification, élément modifié et type de modification effectué.	▪ Assure un enregistrement précis, complet et définitif de toutes les modifications apportées au système.
Identification des sources de modification	Associe chaque modification à sa source : auteur de la modification, séquence des événements l'ayant précédé et processus/programme à l'origine de la modification.	▪ Valide les modifications approuvées, identifie rapidement les modifications non autorisées et augmente le taux de réussite des modifications.

Fonctionnalité	Description	Avantage
Charge opérationnelle faible		
Déploiement simple, sans intervention ultérieure	S'installe en quelques minutes, sans procédure de configuration initiale particulière. Aucune configuration en cours de fonctionnement n'est nécessaire.	▪ Solution immédiatement opérationnelle après l'installation, ne nécessitant aucune maintenance suivie. Économies considérables en termes de charges d'exploitation.
Solution indépendante des applications qui ne nécessite ni signatures, ni règles, ni période d'apprentissage	Solution n'utilisant pas de règles ni de bases de données de signatures, directement opérationnelle pour toutes les applications, et n'exigeant pas de période d'apprentissage.	▪ Ne nécessite qu'une attention minimale de l'administrateur pendant le cycle de vie du serveur. ▪ Protège le serveur jusqu'à ce qu'il bénéficie de patchs ou le serveur dépourvu de patchs, en limitant les dépenses d'exploitation. ▪ Haute efficacité ne dépendant pas de la qualité de règles ou de stratégies.
Faible encombrement et utilisation des ressources limitée	Occupe moins de 20 Mo d'espace disque. N'a aucun impact sur les performances d'exécution des applications.	▪ Nécessite la même capacité de stockage et offre un niveau de performances d'exécution similaire quel que soit le système de production stratégique sur lequel elle est déployée.
Absence de faux positifs ou de faux négatifs	Consigne les activités non autorisées uniquement.	▪ Offre des résultats très précis, ce qui diminue les charges d'exploitation par rapport à d'autres solutions de prévention des intrusions sur l'hôte en réduisant considérablement le temps nécessaire à l'analyse quotidienne/hebdomadaire des journaux. ▪ Améliore l'efficacité des administrateurs et réduit les dépenses d'exploitation.

1. Uniquement disponible sur les plates-formes Microsoft Windows.

McAfee
Together is power.

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