McAfee Integrity Control

Protection des systèmes de points de service contre les applications et les modifications non autorisées

Le logiciel McAfee® Integrity Control™ associe des technologies de listes d'autorisation et de contrôle des modifications de pointe, pour que seules les applications approuvées puissent être exécutées sur les périphériques à fonction fixe, tels que les systèmes de points de service, les guichets automatiques bancaires et les bornes interactives. Il offre aux clients des fonctionnalités de détection continue des modifications tout en bloquant de façon proactive les tentatives de modification non autorisées. McAfee Integrity Control s'appuie en outre sur un modèle d'approbation, de sorte que les mises à jour logicielles émanant de sources autorisées peuvent se poursuivre même sur des systèmes qui sont verrouillés.

Principaux avantages

Visibilité sur les changements et contrôle complets
Surveillez en continu les modifications apportées aux fichiers et répertoires critiques sur tous les systèmes à fonction fixe.

Réduction du coût de possession grâce aux listes d'autorisation dynamiques
Eliminez les tâches manuelles associées à la maintenance des bases de données, des règles et des mises à jour sur les systèmes à fonction fixe.

Mise en œuvre de la stratégie de contrôle des modifications
Assurez-vous que les modifications sont apportées conformément à la stratégie et aux procédures établies.

Transparence des opérations
Aucune charge fonctionnelle supplémentaire ne pèse sur les périphériques à fonction fixe.

Blocage des applications et des tentatives de modification non autorisées

McAfee Integrity Control permet au service informatique de s'assurer que seuls les logiciels autorisés s'exécutent sur l'infrastructure de points de service, sans entraîner une charge fonctionnelle supplémentaire. Il bloque facilement les applications malveillantes, vulnérables ou non autorisées, susceptibles de compromettre l'intégrité des systèmes critiques. Le modèle d'approbation basé sur des listes d'autorisation dynamiques de la solution protège étroitement les systèmes tout en permettant les mises à jour ou modifications autorisées émanant de sources approuvées définies par l'administrateur. Il élimine ainsi le support manuel coûteux associé à d'autres technologies de listes d'autorisation, puisqu'aucune base de données, règle ou mise à jour n'est requise.

Le logiciel McAfee Integrity Control exploite également la technologie de contrôle des modifications, qui permet de bloquer toute modification indésirable et non conforme aux stratégies avant qu'elle n'intervienne. La solution lie directement ce niveau de protection à la stratégie et vérifie la source, la période ou le ticket d'approbation de la modification. Les tentatives de modification non conformes aux stratégies sur les systèmes configurés avec le logiciel sont bloquées et consignées, en plus de générer l'envoi d'une alerte aux administrateurs. Cette approche réduit considérablement les interruptions de service liées aux modifications et les infractions aux règles de conformité.

Surveillance de l'intégrité et des modifications des fichiers

La surveillance de l'intégrité des fichiers permet à McAfee Integrity Control de contrôler les fichiers et les répertoires afin de détecter toute modification apportée au contenu et/ou aux autorisations. Cette surveillance s'exécute en continu dans McAfee Integrity Monitor, ce qui est indispensable pour tester et vérifier la sécurité d'un environnement ou répondre aux exigences de conformité essentielles, notamment celles de la norme PCI DSS (Payment Card Industry Data Security Standard). Le logiciel McAfee Integrity Control propose des informations complètes sur chaque modification, dont l'utilisateur et le programme à l'origine de celle-ci.

Gestion et déploiement centralisés à l'aide de McAfee ePO

L'intégration transparente avec McAfee® ePolicy Orchestrator® (McAfee ePO™) facilite le déploiement de l'agent McAfee Integrity Control, sa gestion et la génération de rapports connexes. La console McAfee ePO unique réduit le coût de possession en consolidant la gestion de la sécurité et de la conformité des périphériques à fonction fixe. Les services informatiques sont ainsi en mesure de réaliser des économies sur les coûts du matériel, de formation et d'exploitation, tout en bénéficiant d'un contrôle unifié sur les stratégies et les mesures de protection appliquées aux guichets automatiques bancaires, aux bornes interactives et aux terminaux de point de vente. Grâce à l'intégration avec la plate-forme McAfee ePO, il n'est plus nécessaire de gérer des données dans deux systèmes distincts.

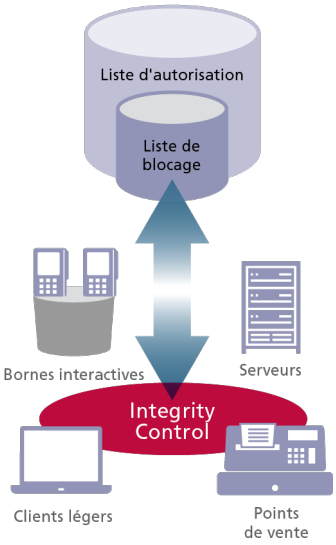

Figure 1. McAfee Integrity Control ajoute un niveau de protection pour les systèmes à fonction fixe tels que les bornes interactives, les terminaux de point de vente et les plates-formes héritées afin de réduire de manière considérable les risques auxquels les clients sont exposés.

Considérations relatives au déploiement

Contrôle renforcé sur les systèmes à fonction fixe — Dans des secteurs fortement réglementés tels que la petite distribution, les services financiers et les soins de santé, les périphériques tels que les terminaux de points de vente, les guichets automatiques bancaires et les systèmes d'imagerie médicale assurent des fonctions critiques et stockent souvent des données sensibles. McAfee Integrity Control est la solution idéale pour offrir un niveau de protection supplémentaire aux systèmes à fonction fixe en termes de ressources mémoire et du processeur. Cette solution sollicite peu de ressources, de sorte qu'elle n'a aucune incidence sur les performances système. En outre, les frais d'investissement et opérationnels sont réduits, sans compter qu'elle est tout aussi efficace en mode autonome sans accès réseau.

Respect et maintien de la conformité à la norme PCI DSS — De nombreux systèmes de points de service tels que les guichets automatiques bancaires, les terminaux de point de vente et les bornes interactives sont tenus d'être en conformité avec la norme PCI DSS. McAfee Integrity Control fournit en continu des informations sur les événements de modifications à l'échelle de l'infrastructure de points de service, notamment sur le ou les serveurs à l'origine de la modification, l'heure et la date de la modification, l'utilisateur responsable, le type de modification et le contenu modifié au sein du fichier, et précise également si la modification a été approuvée. Ce niveau étendu de visibilité dans l'environnement de points de service est possible grâce à la plate-forme McAfee ePO et permet aux services informatiques de vérifier en permanence la sécurité des systèmes de point de vente à des fins de démonstration de leur conformité à la norme PCI DSS auprès des auditeurs.

Amélioration de la disponibilité des services — Les arrêts imprévus des périphériques à fonction fixe ont souvent pour origine des modifications non autorisées ou non testées, et l'essentiel du temps requis pour rétablir la disponibilité de ces systèmes est consacré à l'identification des changements apportés. Cette situation s'explique par le fossé qui sépare l'application pratique des modifications du processus de modification documenté. Cet écart au niveau du contrôle des modifications se traduit par des interventions manuelles de la part du service informatique, qui est tenu de maîtriser et de réduire les coûts élevés liés aux modifications et aux interruptions de service qu'elles provoquent. En comblant ce fossé, McAfee Integrity Control permet aux services informatiques d'accroître la disponibilité des services des périphériques à fonction fixe. Le logiciel surveille les modifications en continu par le biais de la plate-forme McAfee ePO et permet la mise en œuvre sélective de stratégies de modifications afin de prévenir toute modification inconnue avant qu'elle ne cause des problèmes. McAfee Integrity Control aide en outre les clients à réduire le nombre d'incidents d'indisponibilité (mesurés d'après la durée moyenne entre les défaillances), de même que le délai de reprise par incident (calculé sur la base de la durée moyenne de réparation).

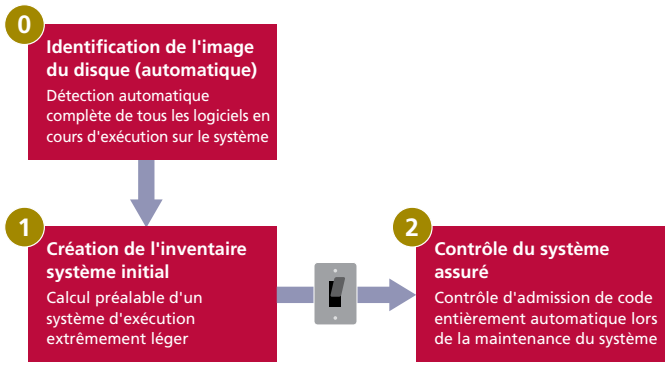

Figure 2 : Fonctionnement des listes d'autorisation dynamiques.

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

7958brf_grc_integrity-control_0110