

# McAfee Change Control

Blocage des modifications non autorisées et automatisation des contrôles de conformité réglementaire

## Principales caractéristiques

- **Contrôle de l'intégrité des fichiers** — Suit en permanence les modifications apportées aux fichiers et aux clés de Registre et identifie la personne responsable ainsi que les fichiers concernés.
- **Blocage des modifications** — Protège les clés de Registre et les fichiers critiques contre les altérations, qui sont autorisées uniquement lorsqu'elles sont conformes aux stratégies de mise à jour.
- **Rapprochement des modifications** — S'intègre avec les systèmes de gestion des modifications pour entreprises via le logiciel McAfee ePolicy Orchestrator® (McAfee ePO™), notamment par une intégration en un clic avec BMC Remedy.

## Faible encombrement et utilisation des ressources réduite

- Configuration aisée et faible charge fonctionnelle initiale et continue
- Utilisation de la mémoire négligeable
- Aucune analyse des fichiers susceptible d'affecter les performances système

À l'heure actuelle, dans de nombreuses entreprises, les environnements de serveur subissent constamment des modifications qui passent le plus souvent inaperçues. C'est une situation dangereuse, tant du point de vue de la sécurité que de la conformité. McAfee® Change Control assure la détection en temps réel et continue des modifications autorisées, à l'échelle de l'entreprise. La solution bloque les tentatives de modifications 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.

Le logiciel McAfee Change Control élimine l'application de modifications dans les environnements serveur, bien trop courantes à l'heure actuelle, susceptibles d'entraîner des compromissions de sécurité, des fuites de données ainsi que des pannes et défaillances. Grâce à ses fonctions de contrôle de l'intégrité des fichiers, de blocage des modifications et à un composant de rapprochement des modifications (en option), McAfee Change Control met en œuvre les stratégies et assure une surveillance permanente des systèmes critiques, alliée à une détection des modifications sur les sites distribués et distants. La solution bloque en outre les tentatives de modifications indésirables.

McAfee Change Control comprend une interface de recherche intuitive qui permet aux utilisateurs de cibler rapidement les informations relatives aux événements de modification. Par exemple, il est possible d'interroger l'interface sur des données concernant toutes les modifications survenues dans le répertoire c:\windows\system32 sur le serveur xyz.acme.com.

## Contrôle de l'intégrité des fichiers de nouvelle génération

Les conditions de la norme PCI DSS 10 et 11.5 concernent le suivi et la surveillance de l'ensemble des accès aux ressources réseau et aux données sur les titulaires de cartes, ainsi que le déploiement d'outils de contrôle de l'intégrité des fichiers, destinés à signaler au personnel toute modification non autorisée des fichiers de contenu, des fichiers de configuration ou des fichiers système stratégiques. McAfee Change Control vous permet d'implémenter un logiciel de contrôle de l'intégrité des fichiers en temps réel et de valider la conformité PCI avec efficacité et rentabilité. Ce contrôle répond aux questions fondamentales *qui, quand, quoi et pourquoi* : la solution indique le nom d'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. Elle peut en outre vous aider à identifier les causes fondamentales d'une interruption de service lors d'une opération de dépannage.

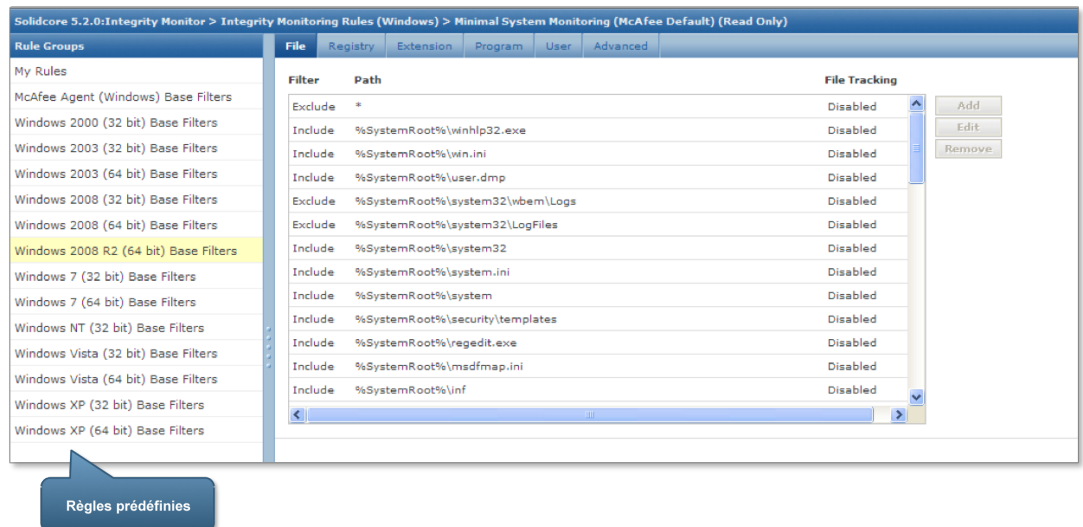


Figure 1. McAfee Change Control comprend des règles prédéfinies pour le contrôle de l'intégrité des fichiers ainsi que des filtres sophistiqués qui permettent de surveiller uniquement les fichiers pertinents.

### Principaux avantages

- Visibilité ininterrompue et gestion en temps réel des modifications des fichiers de contenu, des fichiers de configuration et des fichiers système critiques
- Prévention des modifications des clés de Registre et des fichiers critiques par des tiers non autorisés
- Conformité aux conditions de la norme PCI DSS en ce qui concerne le système de contrôle de l'intégrité des fichiers
- Mise en route facile grâce à des règles prédéfinies pour le contrôle de l'intégrité des fichiers
- Rapports de type QSA pour faciliter la génération de rapports de conformité PCI
- Fonction d'exclusion en un seul clic permettant d'éviter le suivi d'informations non pertinentes
- Mise en œuvre stricte des stratégies grâce au blocage proactif des modifications hors processus et indésirables avant leur application
- Intégration avec la console McAfee ePolicy Orchestrator® (McAfee ePO™) pour une gestion informatique centralisée
- Intégration en un seul clic de McAfee ePO avec BMC Remedy

### Plates-formes prises en charge Microsoft Windows (32 et 64 bits)

- Systèmes embarqués : XPE, 7E
- Systèmes serveur : NT, 2000, 2003, 2003 R2, 2008, 2008 R2
- Postes de travail : XP, Vista, 7

### Linux

- RHEL 3, 4, 5, 6
- Suse 9, 10, 11
- CentOS 4 et 5
- SLED 11
- OpenSUSE 10/11

### Solaris

- 8, 9, 10 sous SPARC
- 10 sous x86, x86-64

### AIX

- AIX 5.3, 6.1

### HPUX

- HPUX 11i v1, v2, v3

Des filtres d'inclusion et d'exclusion peuvent être configurés de sorte que seules les modifications pertinentes et exploitables sont enregistrées. Par ailleurs, des mécanismes d'alerte spéciaux vous informent immédiatement des modifications critiques, pour vous permettre d'éviter les interruptions relatives à la configuration — une des meilleures pratiques recommandées par ITIL (Information Technology Infrastructure Library). Des formulaires QSA (Evalueur 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. Allié au logiciel McAfee Change Reconciliation (en option), McAfee Change Control vous permet de créer un cadre automatisé de contrôles informatiques dans lequel 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, fournissant ainsi un aperçu global de la sécurité d'entreprise. Il vous offre la flexibilité nécessaire pour définir les types ou la sélection de systèmes à couvrir et vous permet de déterminer les fichiers, répertoires et configurations devant faire l'objet d'alertes de modification, ainsi que la priorité des alertes.

Le logiciel propose notamment des profils par défaut pour les systèmes d'exploitation serveur et les applications d'entreprise les plus courants afin de surveiller les composants. Avec McAfee Change Control et McAfee ePO, de nouveaux profils peuvent être activés à tout moment pour renforcer la protection, d'une simple surveillance à une mise en œuvre hypersécurisée.

Le logiciel McAfee ePO est évolutif et facilement extensible. Il intègre le logiciel McAfee Change Control, couplé à d'autres produits de gestion de la sécurité de McAfee, avec les produits de sécurité des partenaires McAfee Security Innovation Alliance. Par ailleurs, lorsque McAfee Change Control est combiné au module logiciel de rapprochement des changements (en option), il fournit une intégration en un seul clic entre McAfee ePO et BMC Remedy.

### Une mise en œuvre stricte pour une efficacité totale

Le logiciel McAfee Change Control suit et valide toute tentative de modification en temps réel sur votre serveur. Le processus de mise en œuvre des stratégies de modification impose que les modifications soient effectuées seulement lors d'une période donnée, par une source fiable ou via un ticket d'approbation. Le composant de blocage des modifications du logiciel McAfee Change Control peut par ailleurs être optimisé pour permettre aux applications natives de mettre à jour leurs fichiers sans interruption, tout en empêchant les autres applications ou utilisateurs de modifier, voire de lire, les fichiers désignés.

### Réduction des risques et optimisation de la conformité sur plusieurs fronts

McAfee offre une vaste gamme de solutions de gestion des risques et de la conformité qui contribuent à réduire les risques, à automatiser la mise en conformité et à optimiser la sécurité. McAfee Change Control et McAfee Application Control se combinent d'ailleurs particulièrement bien pour éliminer les vulnérabilités et assurer la conformité dans toute l'entreprise.

