McAfee Change Control

Verhinderung nicht autorisierter Änderungen und Automatisierung der Kontrolle von Vorschriften-Compliance

Wichtige Funktionen

- *Dateiintegritätsüberwachung* – Überwacht ununterbrochen Veränderungen an Dateien sowie Registrierungsschlüsseln und erfasst den Benutzer, der diese Veränderungen vornimmt
- *Verhinderung von Änderungen* – Schützt kritische Dateien sowie Registrierungsschlüssel vor Manipulation und lässt nur Änderungen zu, die Aktualisierungsrichtlinien entsprechen
- *Änderungsabgleich* – Integriert McAfee Change Control über McAfee ePolicy Orchestrator® (McAfee ePO™) mit Änderungsverwaltungssystemen für Unternehmen, z. B. Ein-Klick-Integration mit BMC Remedy

Geringer Speicherplatzbedarf, geringer Verwaltungsaufwand

- Einfache Einrichtung sowie geringer Aufwand für Einrichtung und Betrieb
- Sehr geringere Speicherauslastung
- Keine Beeinträchtigung der Systemleistung durch Datei-Scans

In Server-Umgebungen ergeben sich in vielen Unternehmen ständig Veränderungen, die unbemerkt bleiben und damit gleichermaßen die Sicherheit und Compliance gefährden. McAfee® Change Control erkennt zulässige Änderungen im gesamten Unternehmen, sobald diese auftreten. Die Lösung blockiert nicht autorisierte Änderungen an wichtigen Systemdateien, Verzeichnissen und Konfigurationseinstellungen und vereinfacht gleichzeitig die Implementierung neuer Richtlinien und Compliance-Maßnahmen.

Die Software McAfee Change Control verhindert Änderungen, die in Unternehmen sehr verbreitet sind und zu Sicherheitsverletzungen, Datenverlusten und Systemausfällen führen können. Mit Funktionen zur Dateiintegritätsüberwachung, Verhinderung von Änderungen und einer optionalen Komponente für den Änderungsabgleich setzt McAfee Change Control Änderungsrichtlinien um und ermöglicht die kontinuierliche Überwachung wichtiger Systeme sowie die Erkennung von Veränderungen auch an verteilten und entfernten Standorten. Gleichzeitig werden unerwünschte Änderungen blockiert.

Über die intuitive Suchoberfläche von McAfee Change Control können Benutzer schnell Detailinformationen zu Änderungsereignissen abrufen. So können Sie zum Beispiel Daten zu allen Änderungen im Verzeichnis c:\windows\system32 abfragen, die auf dem Server xyz.acme.com vorgenommen wurden.

Dateiintegritätsüberwachung der nächsten Stufe

Die PCI DSS-Anforderungen 10 und 11.5 verlangen die Nachverfolgung und Überwachung aller Zugriffe auf Netzwerk-Ressourcen und Karteninhaberdaten sowie den Einsatz von Dateiintegritätsüberwachungs-Tools, mit denen Mitarbeiter bei nicht autorisierten Änderungen an wichtigen System-, Konfigurations- oder Inhaltsdateien benachrichtigt werden können. McAfee Change Control stellt eine Dateiintegritätsüberwachung in Echtzeit bereit und ermöglicht, die PCI-Compliance effizient und kostengünstig zu validieren. Die Dateiintegritätsüberwachung von McAfee Change Control liefert zentral und in Echtzeit wichtige Informationen dazu, wer wann was und warum geändert hat, d. h. den Benutzernamen, den Zeitpunkt der Änderung, den Programmnamen sowie Daten zur betroffenen Datei bzw. zum Registrierungsschlüssel. Außerdem erhalten Sie bei einem Systemausfall Unterstützung bei der Identifizierung des Kernproblems.

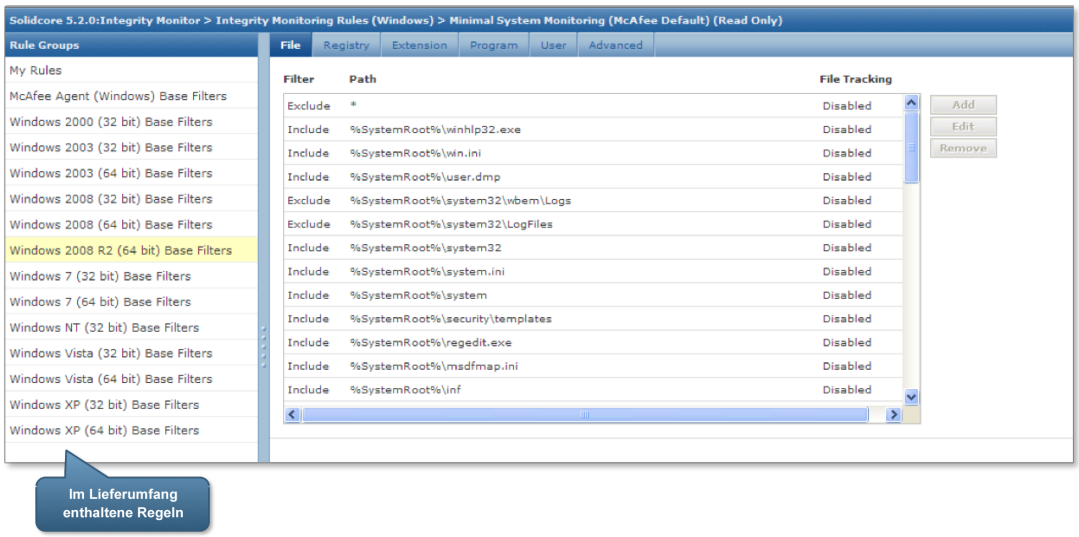

Abbildung 1. McAfee Change Control beinhaltet vorkonfigurierte Regeln für die Dateiintegritätsüberwachung sowie erweiterte Filter zur Überwachung ausschließlich relevanter Dateien.

Hauptvorteile

- Kontinuierlicher Überblick und Echtzeitverwaltung der Änderungen an wichtigen System-, Konfigurations- und Inhaltsdateien
- Verhinderung der Manipulation wichtiger Dateien und Registrierungsschlüssel durch Unbefugte
- Einhaltung der PCI DSS-Vorschriften durch Dateiintegritätsüberwachung
- Schnelle Einrichtung dank bereits im Lieferumfang enthaltener Regeln für die Dateiintegritätsüberwachung
- QSA-freundliche Berichte zum einfachen Nachweis der PCI-Compliance
- Funktion mit Ein-Klick-Ausschluss, um irrelevante Informationen aus der Überwachung auszuschließen
- Strenge Richtlinienerzwingung durch präventive Blockierung prozessexterner oder unerwünschter Änderungen, bevor sie vorgenommen werden
- Integration mit der McAfee ePolicy Orchestrator® (McAfee ePO™)-Konsole zur zentralen IT-Verwaltung
- Ein-Klick-Integration über McAfee ePO mit BMC Remedy

Unterstützte Plattformen

Microsoft Windows (32- und 64-Bit-Versionen)

- Eingebettet: XPE, 7E
- Server: NT, 2000, 2003, 2003 R2, 2008, 2008 R2
- Desktop: Windows XP, Vista, 7

Linux

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

Solaris

- 8, 9, 10 (SPARC)
- 10 (x86, x86-64)

AIX

- AIX 5.3, 6.1

HPUX

- HPUX 11i v1, v2, v3

Filter zum Einschließen/Ausschließen können so konfiguriert werden, dass nur relevante sowie solche Änderungen erfasst werden, die Aktionen erfordern können. Darüber hinaus werden Sie über einen speziellen Warnmeldungsmechanismus sofort über schwerwiegende Änderungen informiert, damit Sie Ausfälle durch Konfigurationsänderungen vermeiden können. Diese Vorgehensweise wird von der Information Technology Infrastructure Library (ITIL) empfohlen. Zur Vereinfachung von PCI-Berichten stehen QSA-Formulare (Qualified Security Assessor) zur Verfügung.

Verhinderung von Systemausfällen aufgrund ungeplanter Änderungen

McAfee Change Control erlaubt IT-Mitarbeitern die einfache Behebung von Zwischenfällen, Automatisierung der Kontrolle von Vorschriften-Compliance und Vermeidung von änderungsbedingten Systemausfällen. Dank McAfee Change Control benötigen Sie keine manuellen, fehleranfälligen und Ressourcen-intensiven Compliance-Richtlinien, die häufig aufgrund der Anforderungen des US-Aktiengesetzes Sarbanes-Oxley (SOX) implementiert werden. In Verbindung mit der Änderungsabgleich-Software McAfee Change Reconciliation (optional) ermöglicht McAfee Change Control die Einrichtung eines automatisierten IT-Steuerungs-Frameworks, in dem alle für die Compliance-Validierung erforderlichen Informationen über ein zentrales Berichterstellungssystem abgerufen werden können. Die Validierung autorisierter Änderungen erfolgt automatisch. Notfall-Patches und andere prozessexterne Änderungen werden automatisch dokumentiert und zur leichteren Überprüfung abgeglichen.

Zentralisiertes Sicherheits- und Compliance-Management

McAfee ePolicy Orchestrator® (McAfee ePO™) konsolidiert sowie zentralisiert die Verwaltung und bietet einen globalen Überblick über die Unternehmenssicherheit. Sie können die zu überprüfenden System-Arten oder -Bereiche flexibel anpassen und festlegen, welche Dateien, Verzeichnisse und Konfigurationen mit welcher Priorität bei Änderungswarnmeldungen berücksichtigt werden sollen. Es sind Standardprofile verfügbar, die für die gängigsten Varianten von Server-Betriebssystemen und Unternehmensanwendungen entwickelt wurden und zur Überwachung wichtiger Komponenten herangezogen werden können. In diesen Fällen müssen keine Profile von Grund neu erstellt werden. Mit McAfee Change Control und der Software McAfee ePO können neue Profile jederzeit aktiviert werden, um den Schutz von einfacher Überwachung bis zur absolut sicheren Schutzmauer zu erhöhen.

McAfee ePO kann skaliert und einfach erweitert werden. Die Lösung integriert die McAfee Change Control-Software und andere McAfee-Sicherheitsverwaltungsprodukte mit Produkten von McAfee Security Innovation Alliance-Partnern. In Kombination mit der optionalen Änderungsabgleich-Software bietet McAfee Change Control eine Ein-Klick-Integration zwischen McAfee ePO und BMC Remedy.

Erzwingung ändert alles

Die Software McAfee Change Control überwacht und validiert in Echtzeit alle Änderungsversuche auf Ihrem Server. Sie erzwingt Änderungsrichtlinien, indem sie Änderungen nur innerhalb eines Zeitfensters, von vertrauenswürdigen Quellen oder genehmigten Ablauf-Tickets zulässt. Die Änderungsschutz-Komponente von McAfee Change Control kann so optimiert werden, dass systemeigene Anwendungen ihre Dateien weiterhin ohne Unterbrechung aktualisieren können, während alle anderen Anwendungen oder Benutzer keine Änderungen durchführen dürfen oder sogar am Lesen dieser Dateien gehindert werden.

Minimales Risiko und maximale Rendite an mehreren Fronten

McAfee bietet verschiedenste Risiko- und Compliance-Lösungen an, die Sie bei der Risikominimierung, der Automatisierung der Compliance und der Sicherheitsoptimierung unterstützen. Hierbei stellen McAfee Change Control und McAfee Application Control eine leistungsfähige Kombination zur Schwachstellenminimierung dar, mit der Sie die Compliance im gesamten Unternehmen gewährleisten können.

McAfee
An Intel Company

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

McAfee, das McAfee-Logo, McAfee ePolicy Orchestrator und McAfee ePO sind Marken oder eingetragene Marken von McAfee, Inc. oder der Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Die in diesem Dokument enthaltenen Produktpläne, Spezifikationen und Beschreibungen dienen lediglich Informationszwecken, können sich jederzeit ohne vorherige Ankündigung ändern und schließen alle ausdrücklichen oder stillschweigenden Garantien aus. Copyright © 2012 McAfee, Inc.
41100ds_mcc_1211_fnl_ETMG