

# McAfee Change Control

## Kontinuierlicher Schutz vor nicht autorisierten Änderungen



In vielen IT-Unternehmen besteht eine Lücke zwischen autorisierten und dokumentierten Änderungen und den tatsächlichen Änderungsvorgängen. Bei Unternehmen, die mehreren Compliance-Vorschriften unterliegen, kann die Möglichkeit zur Überwachung von Datei- und Konfigurationsänderungen und der zentralen Durchsetzung der Einhaltung von Richtlinien für die Autorisierung von Änderungen für eine höhere Verfügbarkeit und verifizierbare Compliance sorgen. McAfee® Change Control ist vollständig in die McAfee ePolicy Orchestrator® (McAfee ePO™)-Verwaltungsplattform integriert. Dies ist die einzige Konsole zur Festlegung von Änderungsrichtlinienprofilen, in der Benachrichtigungen für Änderungsvorfälle und deren Priorisierung angegeben werden können, um eine äußerst effiziente Verwaltung zu gewährleisten. Für kritische Systemkomponenten, Dateien oder Konfigurationseinstellungen bietet McAfee vollständigen Schutz vor nicht autorisierten Änderungen.

Die meisten IT-Unternehmen investieren in Tools zur Prozessautomatisierung wie ein Änderungsverwaltungssystem oder einen Service Desk. Dennoch gibt es eine Lücke zwischen der tatsächlichen Änderungsaktivität und dem dokumentierten Änderungsverwaltungsprozess oder der festgelegten Richtlinie. Diese Lücke bei der Änderungskontrolle führt seitens der IT-Abteilungen zu einem Übermaß an manuellen Aktivitäten, wenn es darum geht, Audits zu unterstützen und Ereignisse durch die manuelle Überprüfung der tatsächlichen Änderungen auf Systemebene mit dem Arbeitsauftrag oder Trouble-Ticket für die angeforderte Änderung abzugleichen. Zudem werden Ad-hoc-Änderungen oftmals ohne Verifizierung und Validierung durchgeführt und führen somit möglicherweise zu einer Beeinträchtigung der Konfigurationseinstellungen für die Systemsicherheit. Dies kann wiederum eine Abweichung von den Unternehmensrichtlinien oder Auswirkungen auf die Leistung und Verfügbarkeit von Servern nach sich ziehen. McAfee Change Control minimiert die Kosten von Änderungen, da es ein zentralisiertes oder vorab festgelegtes Vertrauensmodell (Zeitfenster für die Änderung, Urheber der Änderung oder genehmigter Benutzer) für autorisierte Änderungen durchsetzt und überdies eine fortlaufende Überwachung der Dateiintegrität bietet.

Über die McAfee ePO-Verwaltungskonsole haben Unternehmen die Möglichkeit, den Typ oder Umfang der betreffenden Systeme flexibel

anzupassen. Sie können auch bestimmen, welche Dateien, Verzeichnisse oder Konfigurationen in Änderungswarnungen aufgenommen werden sollen, sowie die Priorität der Warnungen festlegen. Es sind Standardprofile verfügbar, die für die gängigsten Typen von Server-Betriebssystemen und Unternehmensanwendungen entwickelt wurden und zur Überwachung für kritische Komponenten herangezogen werden können. In diesen Fällen müssen keine Profile von Grund neu erstellt werden. Zu jedem Zeitpunkt kann ein neues Profil aktiviert werden, das von der einfachen Überwachung bis hin zur Durchsetzung verbesserten Schutz bietet. Dabei werden Änderungen an Dateien, Verzeichnissen oder Konfigurationen verhindert – es sei denn, sie werden von vertrauenswürdigen Quellen initiiert. Der Schutz vor Änderungen kann so optimiert werden, dass systemeigene Anwendungen ihre Dateien weiterhin ohne Unterbrechung aktualisieren können, alle anderen Anwendungen oder Benutzer aber keine Änderungen durchführen dürfen oder durch die Lese-/Schreibschutzfunktion von McAfee Change Control sogar am Lesen dieser Dateien gehindert werden.

McAfee Change Control bietet Unternehmen die kontinuierliche Ermittlung von Änderungen, die über verteilte und entfernte Standorte hinweg vorgenommen werden, sowie Schutzmaßnahmen, durch die unerwünschte Änderungen blockiert werden können. McAfee Change Control schließt die Lücke für Unternehmen, da es ihnen die IT-Steuermechanismen für ihre Änderungsverwaltung

zur Verfügung stellt. Mithilfe dieser Lösung können IT-Abteilungen PCI- und SOX-Steuermechanismen problemlos für Compliance-Zwecke automatisieren. Zudem werden änderungsbedingte Ausfälle verhindert, sodass die Serviceverfügbarkeit verbessert und die Information Technology Infrastructure Library (ITIL) schneller angewendet werden kann. McAfee Change Control ist eine leicht bedienbare und benutzerfreundliche Lösung mit geringem Verwaltungsaufwand, die auf einer Vielzahl von Server-Hardware-Plattformen bereitgestellt werden kann.

### Kontinuierliche Änderungskontrolle

Im Gegensatz zu Scan-basierten Lösungen, die Momentaufnahmen eines Systems erstellen und vergleichen, überwacht und validiert McAfee Change Control kontinuierlich jeden Änderungsversuch am Server in Echtzeit. Als Grundlage wird ein definiertes Änderungskontrollprofil verwendet.

McAfee Change Reconciliation, das zusammen mit McAfee Change Control eingesetzt werden kann, korreliert die auf Servern vorgenommenen Änderungen mit den dokumentierten Änderungstickets vorhandener Ticket-Systeme und lässt sich mit beliebigen Änderungsverwaltungssystemen wie HP Service Manager und BMC Remedy verknüpfen. Darüber hinaus ist es möglich, McAfee auch in beliebige Konfigurationsmanagement-Datenbanken wie BMC Atrium und HP Universal CMDB zu integrieren. Änderungsinformationen, die Bestandteil des Trouble-Tickets oder Arbeitsauftrags sind, werden zusammengefasst und in das Ticket-System integriert, wodurch Unternehmen nicht nur den Workflow, sondern auf Systemebene auch Details zur geleisteten Arbeit verfolgen können.

McAfee Integrity Monitor wurde auch zur Erweiterung von McAfee Change Control entwickelt. Damit ist es schnell und einfach möglich, die Anforderungen an die Audit-Protokolle zu Datenbank- und Netzwerkgeräten zu erfüllen, die in vielen Compliance-Standards wie PCI DSS festgelegt sind. Dank der Berichtsfunktionen der McAfee ePO-Verwaltungskonsole können Administratoren alle Änderungen an Servern und den zusätzlichen Datenbank- und Netzwerkgeräten anzeigen und sich so einen Überblick darüber verschaffen, wo Compliance-Richtlinien verletzt werden. Die Lösung erkennt vorübergehende Verstöße wie unangemessene und wieder zurückgenommene Dateiänderungen und erstellt entsprechende Warnmeldungen. Außerdem erfasst sie die spezifischen Daten zu jeder Änderung, einschließlich der genauen Uhrzeit.

### Unternehmenslösungen

#### Einhaltung und Durchsetzung der PCI DSS-Vorschriften

Die Einhaltung der Vorschriften des Payment Card Industry Data Security Standard (PCI DSS) verpflichtet Händler und Service Provider, ca. 180 verschiedene Anforderungen in 12 Kategorien zu erfüllen. Jüngste Forschungen haben allerdings gezeigt, dass die Anforderungen der Kategorien 10 und 11, die die Überwachung der Dateiintegrität und die Audit-Protokolle behandeln, am schwierigsten zu erfüllen sind und am seltensten erfüllt werden. Diesen Anforderungen ist schwer nachzukommen, weil bisherige Tools nur eine „periodische“ Überwachung der Dateiintegrität bieten, die Änderungen über ressourcenintensive System-Scans erkennen. McAfee Change Control bietet eine kategorische Kontrolle der IT-Infrastruktur, die es Einzelhändlern und anderen, die Kreditkartentransaktionen durchführen, ermöglicht, die schwierigen PCI-Anforderungen zu erfüllen und PCI-Compliance effizient und kostengünstig nachzuweisen.

Um Unternehmen aller Größen die einfache und kostengünstige Erfüllung der Anforderungen hinsichtlich der Dateiintegritätsüberwachung und der Audit-Protokolle gemäß der Abschnitte PCI DSS 1, 10 und 11 zu ermöglichen, bieten wir McAfee Change Control und McAfee Integrity Monitor an. Viele weltweit führende qualifizierte Sicherheitsgutachter bestätigen und empfehlen diese Lösungen als wesentliches Element einer umfassenden PCI-Compliance-Strategie.

#### Sarbanes-Oxley und IT-Steuermechanismen für andere Compliance-Vorschriften

Der Sarbanes-Oxley Act (SOX, US-Gesetz für Aktiengesellschaften mit Sitz in den USA) bildete den Beginn einer grundlegenden Verschiebung in der Unternehmensführung. Mittlerweile müssen Unternehmen durchschnittlich vier Compliance-Standards einhalten. Bei der Bewältigung der Implikationen der mehrschichtigen Compliance-Anforderungen wird eines klar: Compliance ist kein einmaliges Projekt, sondern ein ständiges Bemühen um Transparenz und Verantwortlichkeit für Geschäftsprozesse und Sicherheit. Zur Erfüllung dieser überaus strengen Compliance-Anforderungen haben viele Unternehmen Compliance-Richtlinien implementiert, die manuell umgesetzt werden müssen, fehleranfällig und ressourcenintensiv sind.

McAfee Change Control hat einer Reihe von Kunden bei der Bewältigung der komplexen Compliance-Herausforderungen geholfen, da es mit McAfee Change Reconciliation ein eigenständiges, automatisiertes Framework für die IT-Steuerung bildet, in dem alle zur Überprüfung der Compliance erforderlichen Informationen in einem einzigen Berichtssystem verfügbar sind. Die von McAfee angebotene Änderungserkennung mit ihrem automatischen und äußerst präzisen Änderungsabgleich bietet anhand von Berechtigungen die automatische Validierung von Änderungen. Prozessexterne Änderungen (z. B. Notfall-Patches) werden automatisch dokumentiert und zur leichteren Überprüfung abgeglichen. Kunden, die McAfee Change Control für Sarbanes-Oxley-Audits nutzen, genießen beträchtliche Vorteile – sowohl in Form der Risiko- als auch der Kostenreduzierung. In den meisten Fällen zeigen sich die Vorteile zunächst bei der Automatisierung bestehender manueller Kontrollen und dann bei der Rationalisierung und Reduzierung der Kontrollen. Dies wird durch den Nachweis für Auditoren ermöglicht, dass die Kontrollfunktionen in die Struktur eingebettet sind.

### Optimierung von Sicherheit und Compliance

Die meisten mittelständischen und großen Unternehmen suchen nach Möglichkeiten, ihre Betriebseffizienz im Hinblick auf Sicherheit und Compliance zu verbessern. Ohne Änderungskontrolle erzielen alle Investitionen in die Automatisierung und die Effizienz schlechtere Renditen als möglich wäre, weil sie sich im Wesentlichen auf ein bewegliches Ziel richten. Die größte Hürde für erfolgreiche Projekte ist der Nachweis einer Rendite für das Unternehmen, insbesondere da es sich bei Projekten zumeist um große, mehrphasige Implementierungen handelt. Kunden nutzen McAfee Change Control, um die Zeitspanne bis zum Nachweis der Rendite für das Unternehmen drastisch zu verkürzen und ein höheres Maß an IT-Haftbarkeit zu erlangen. McAfee Change Control sorgt für eine kontinuierlich kontrollierte Umgebung, die die Automatisierung unterstützt. Die Kunden erhalten Einblick in Änderungen und mit der McAfee ePO-Verwaltungsplattform eine zentrale Konsole, die mit sofortiger Wirkung eine gezielte Durchsetzung von Änderungsrichtlinien auf lokalen und verteilten Servern ermöglicht.

