

# McAfee Change Control

## 무단 변경 방지 규정 컴플라이언스 제어 자동화

오늘날 서버 환경의 변화는 여러 조직에서 지속적으로 일어나고 있지만 탐지되고 있지 않습니다. 이는 보안 및 컴플라이언스 측면에서 모두 위험한 상황입니다. McAfee 제품의 일부인 McAfee® Change Control은 허가된 변경 발생 시 기업 전체에서 이러한 변경을 지속적으로 탐지합니다. 중요한 시스템 파일, 디렉터리 및 구성에 대한 무단 변경을 차단하고 동시에 새로운 정책 및 컴플라이언스 대책 구현을 능률화합니다.

McAfee Change Control 소프트웨어는 오늘날의 기업 환경에서 너무나 흔하게 발생하는 변경 활동을 억제합니다. 보안 위반, 데이터 유실 및 중단을 발생시킬 수 있는 활동을 변경합니다. 파일 무결성 모니터링 및 변경 방지 기능을 탑재한 McAfee Change Control은 변경 정책을 시행하며 중요한 시스템에 대한 지속적인 모니터링을 제공합니다. 또한 분산 및 원격 위치 전반에서 발생한 변경 사항을 탐지하며 원치 않는 변경을 차단합니다.

McAfee Change Control은 직관적인 검색 인터페이스를 통해 사용자가 변경 이벤트 정보를 빠르게 확인할 수 있도록 지원합니다. 예를 들어 인터페이스에서 서버 xyz.acme.com에서 만들어진 c:\windows\system32 디렉터리에 대해 변경한 모든 내용에 대한 데이터를 쿼리할 수 있습니다.

### 다음 수준의 파일 무결성 모니터링

PCI DSS (Payment Card Industry Data Security Standard) 요구 사항 10 및 11.5는 네트워크 리소스 및 카드 소유자 데이터에 대한 모든 액세스를 추적 및 모니터링하고, 중요한 시스템, 구성 및 콘텐츠 파일에 대한 무단 수정을 담당자에게 알리는 FIM (파일 무결성 모니터링) 도구를 배포할 것을 호출합니다. McAfee Change Control을 사용하면 실시간 FIM 소프트웨어를 구현하고 경제적이고 효율적인 방식으로 PCI 컴플라이언스를 검증할 수 있습니다. McAfee Change Control FIM은 필수 정보인 변경자, 변경 시점, 변경 항목 및 변경 이유를 파악하여 제공합니다. 또한 사용자 이름, 변경 시간, 프로그램 이름 및 파일/레지스트리 콘텐츠 데이터를 하나의 위치에서 실시간으로 제공합니다. 이에 더하여 중단 이벤트 문제 해결 시 근본 원인을 파악할 수 있도록 지원합니다.

### 주요 기능

- **파일 무결성 모니터링:** 파일 및 레지스트리 키에 대한 변경을 지속적으로 추적하고 어떤 파일을 누가 변경했는지 파악합니다.
- **변경 방지:** 중요한 파일 및 레지스트리 키가 변경되지 않도록 방지합니다. 업데이트 정책에 따라 허가된 변경만 허용합니다.

### 적은 풋프린트 및 낮은 간접 비용

- 설치가 쉽고 초기 및 지속적인 운영 간접 비용이 낮음
- 적은 메모리 사용
- 시스템 성능에 영향을 줄 수 있는 파일 검색 없음

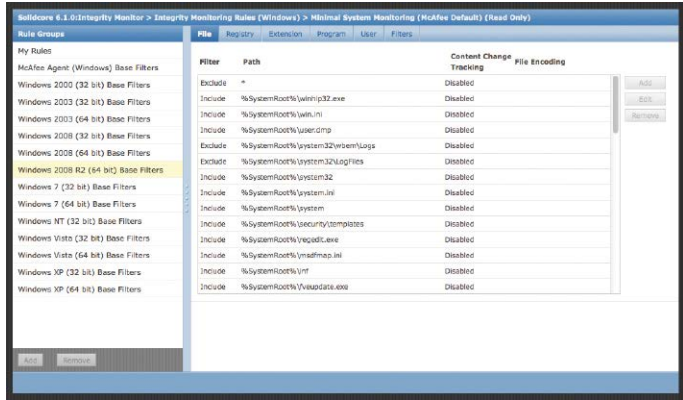


그림 1. 관련된 파일만 모니터링할 수 있도록 기본 제공되는 McAfee Change Control의 FIM 규칙 및 정교한 필터.

### 콘텐츠 변경 추적

McAfee Change Control을 이용하면 파일 콘텐츠와 속성 변경을 추적할 수 있습니다. 파일 콘텐츠 변경에서는 데이터를 서로 비교해 보면서 비교하여 추가되거나 삭제되거나 수정된 사항을 찾을 수 있습니다. 이 기능은 구성 관련 중단 문제를 해결할 때 유용합니다.

관련된 조치 가능한 변경 내용만 캡처하도록 포함/제외 필터를 구성할 수 있습니다. 뿐만 아니라 특수 경보 메커니즘을 통해 중요한 변경 사항을 즉시 알리므로 구성 관련 중단을 방지할 수 있습니다(권장되는 ITIL (정보 기술 인프라 라이브러리) 모범 사례). 간단한 PCI 보고를 위해 QSA (Qualified Security Assessor) 양식이 제공됩니다.

### 예상치 못한 변경으로 인한 중단 방지

McAfee Change Control을 통해 IT 부서에서는 쉽게 사고를 해결하고, 규정 컴플라이언스 제어를 자동화하며, 변경 관련 중단을 방지할 수 있습니다. 또한 McAfee Change Control을 사용하면 일반적으로 SOX (Sarbanes-Oxley) 법과 관련된 오류가 발생할 가능성이 높고 리소스를 많이 사용하는 수동 컴플라이언스 정책이 필요하지 않습니다. McAfee Change Control을 사용하면 단일 보고 시스템에서 컴플라이언스 검증에 필요한 모든 정보를 사용할 수 있는 자동화된 IT 제어 프레임워크를 구축할 수 있습니다. 인증에 대한 변경 내용을 자동으로 검증할 수 있습니다. 보다 용이한 감사를 위해 긴급 수정 및 기타 예기치 못한 변경이 자동으로 문서화되고 조정됩니다.

### 중앙 집중식 보안 및 컴플라이언스 관리

McAfee ePO 소프트웨어는 관리 기능을 통합하고 중앙 집중화하므로 기업 보안에 대한 전체적인 파악이 가능합니다. 즉 포함할 시스템의 유형 또는 범위를 유연하게 조정하고 변경 경보에 포함해야 할 파일, 디렉터리 및 구성과 경보 우선 순위를 결정할 수 있습니다. 가장 일반적인 유형의 서버 운영 체제 및 기업 응용프로그램을 위해 개발된 기본 프로파일을 사용하여 새로운 프로파일을 처음부터 만들지 않고 중요한 구성요소를 모니터링할 수 있습니다. McAfee Change Control과 McAfee ePO 소프트웨어를 사용하면 시간에 관계없이 새 프로파일을 활성화하여 단순한 모니터링부터 완전한 시행에 이르기까지 보안을 향상시킬 수 있습니다.

### 주요 이점

- 중요한 시스템, 구성 또는 콘텐츠 파일에 대한 변경 내용에 대한 지속적인 가시성 및 실시간 관리 제공
- 권한이 없는 사용자가 중요한 파일 및 레지스트리 키를 변경하지 못하도록 방지
- 파일 무결성 모니터링 시스템에 대한 PCI DSS 규정 요구사항 이행 지원
- 기본 제공되는 FIM 규칙을 사용한 손쉬운 시작
- 손쉬운 PCI 보고를 위한 QSA용 보고서
- 관련 없는 정보 추적을 피하기 위한 원클릭 제외 기능
- 예기치 않거나 원치 않는 변경이 발생하기 전에 사전에 차단하여 엄격한 정책 시행
- 중앙 집중화된 IT 관리를 위한 McAfee® ePolicy Orchestrator® (McAfee ePO™) 콘솔과의 통합

McAfee ePO 소프트웨어는 쉽게 확장할 수 있습니다. McAfee Change Control 소프트웨어 및 기타 McAfee 보안 관리 제품을 파트너의 보안 관리 제품과 통합합니다.

### 모든 것을 변경하는 시행

McAfee Change Control 소프트웨어는 서버에서 시도된 모든 변경을 실시간으로 추적 및 검증합니다. 기간 이내에 신뢰할 수 있는 소스에 의한 변경 또는 승인된 작업 티켓을 사용한 변경만 이루어지도록 요구하여 변경 정책을 시행합니다. McAfee Change Control 소프트웨어의 변경 방지 구성요소를 세부적으로 조정하여 다른 모든 응용프로그램 또는 사용자가 변경하거나 지정한 파일을 읽지 못하게 하면서 기본 응용프로그램이 중단 없이 파일을 계속 업데이트하게 할 수 있습니다.

### 여러 프론트에서 위험 최소화 및 컴플라이언스 극대화

McAfee는 위험을 최소화하고, 컴플라이언스를 자동화하며, 보안을 최적화할 수 있도록 광범위한 위험 및 컴플라이언스 솔루션을 제공합니다. 특히 McAfee Change Control과 McAfee Application Control은 기업 전체에서 취약성을 없애고 컴플라이언스를 보장하기에 매우 뛰어난 조합입니다.

### 다음 단계

McAfee Change Control 소프트웨어는 보안 위반, 데이터 유출 및 중단을 발생시킬 수 있는 서버 환경의 변경 활동을 제거하며 규정 컴플라이언스 요구 사항을 손쉽게 충족할 수 있도록 지원합니다. 지금 McAfee Change Control로 규정 컴플라이언스 제어 자동화를 수행하면서 무단 변경을 방지해 보십시오.

### 지원되는 플랫폼

#### Microsoft Windows (32비트 및 64비트)

- 포함: Windows XPE, 7E, WEPOS, Pos Ready 2009, WES 2009
- 서버: Windows NT, 2000, 2003, 2003 R2, 2008, 2008 R2, 2012
- 데스크톱: Windows XP, Vista, 7

#### Linux

- RHEL 5, 6
- Suse 10, 11
- CentOS 5, 6
- OEL 5, 6
- SLED 11
- OpenSUSE 10/11

#### AIX

- AIX 6.1, 7.1



McAfee (Singapore) Pte Ltd  
10 Kallang Avenue #08-10  
Aperia Tower 2  
Singapore 339510  
[www.mcafee.com/kr](http://www.mcafee.com/kr)

McAfee 및 McAfee 로고, ePolicy Orchestrator 및 McAfee ePO는 미국 및 기타 국가에서 McAfee, LLC 또는 자회사의 등록 상표 또는 상표입니다. 기타 이름 및 브랜드는 각 소유자의 재산으로 주장될 수 있습니다. Copyright © 2017 McAfee, LLC. 60736ds\_mcc\_1213B  
2013년 12월