McAfee
An Intel Company

McAfee Change Control

Prevent unauthorized changes while automating regulatory compliance controls.

Key Features

- *File integrity monitoring*— Continuously tracks changes to file and registry keys and identifies who made changes to which files
- *Change prevention*— Protects critical files and registry keys from tampering, with changes only permitted in accordance with update policies
- *Change reconciliation*— Integrates McAfee Change Control with enterprise change management systems through McAfee ePolicy Orchestrator® (McAfee ePO™) software, including single-click integration with BMC Remedy

Small Footprint and Low Overhead

- Easy setup and low initial and ongoing operational overhead
- Negligible memory usage
- No file scanning that could impact system performance

Changes in server environments are constantly taking place in many organizations today—and going undetected. It's a situation that is dangerous, both in terms of security and compliance. McAfee® Change Control delivers continuous, enterprise-wide detection of authorized changes as they occur. It blocks unauthorized changes to critical system files, directories, and configurations while streamlining the implementation of new policies and compliance measures.

McAfee Change Control software eliminates change activity that is far too common in enterprises today—activity that can lead to security breaches, data loss, and outages. Featuring file integrity monitoring, change prevention, and an optional change reconcilation component, McAfee Change Control enforces change policies and provides continuous monitoring of critical systems and detection of changes made across distributed and remote locations. And it blocks unwanted changes.

McAfee Change Control includes an intuitive search interface to help users quickly home in on change event information. For example, you can query the interface for data on all changes that occurred in the c:\windows\system32 directory that were made on the server xyz.acme.com.

Next-Level File Integrity Monitoring

PCI DSS Requirements 10 and 11.5 call for tracking and monitoring all access to network resources and cardholder data and deploying file integrity monitoring (FIM) tools to alert personnel to unauthorized modifications of critical system, configuration, or content files. McAfee Change Control enables you to implement real-time FIM software and validate PCI compliance in an efficient, cost-effective manner. McAfee Change Control FIM provides the who, when, what, and why essentials. It gives you the user name, time of change, program name, and file/registry content data all in one place and all in real time. In addition, it can help you identify root causes when troubleshooting in the event of an outage.

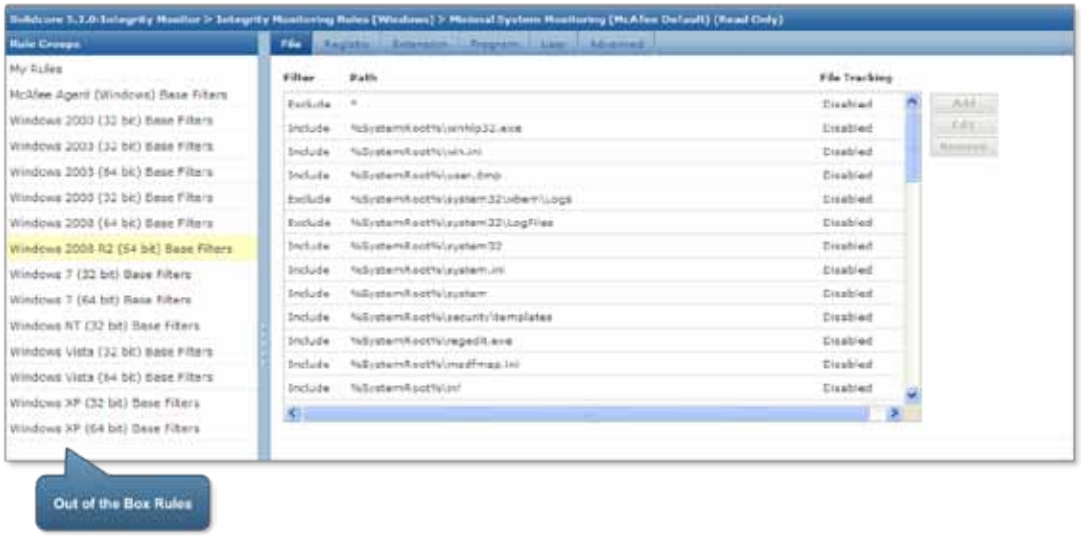

Figure 1. McAfee Change Control features out-of-the-box FIM rules and sophisticated filters for monitoring only relevant files.

Key Advantages

- Gain continuous visibility and real-time management of changes to critical system, configuration, or content files
- Prevent tampering with critical files and registry keys by unauthorized parties
- Fulfill the PCI DSS regulation requirement for file integrity monitoring system
- Easy to get started with out-of-the-box FIM rules
- QSA-friendly reports for easy PCI reporting
- One-click exclusion feature to avoid tracking irrelevant information
- Tight policy enforcement via proactively blocking of out-of-process and unwanted changes before they occur
- Integrates with McAfee ePolicy Orchestrator® (McAfee ePO™) console for centralized IT management
- Single-click McAfee ePO integration with BMC Remedy

Supported Platforms

Microsoft Windows (32-bit and 64-bit)

- Embedded: XPE, 7E
- Server: NT, 2000, 2003, 2003 R2, 2008, 2008 R2
- Desktop: 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 on SPARC
- 10 on x86, x86-64

AIX

- AIX 5.3, 6.1

HPUX

- HPUX 11i v1, v2, v3

Include/exclude filters can be configured so that only relevant, actionable changes are captured. What's more, special alerting mechanisms instantly notify you of critical changes, so you can prevent configuration-related outages—a recommended Information Technology Infrastructure Library (ITIL) best practice. And Qualified Security Assessor (QSA) forms are provided for easy PCI reporting.

Prevent Outages Resulting from Unplanned Changes

McAfee Change Control allows IT to easily resolve incidents, automate regulatory compliance controls, and prevent change-related outages. Moreover, McAfee Change Control can eliminate the need for manual, error-prone, and resource-intensive compliance policies that are often associated with Sarbanes-Oxley (SOX) mandates. In conjunction with McAfee Change Reconciliation software (optional), McAfee Change Control enables you to build an automated IT control framework in which all the information required to verify compliance is available in a single reporting system. Changes against authorizations can be validated automatically. Emergency fixes and other out-of-process changes are automatically documented and reconciled for easier audits.

Centralized Security and Compliance Management

McAfee ePolicy Orchestrator® (McAfee ePO™) software consolidates and centralizes management, providing a global view of enterprise security. It gives you the flexibility to adjust the types or scope of systems to cover and lets you determine which files, directories, and configurations should be included in change alerts, as well as the priority of alerts. Default profiles developed for most common types of server operating systems and enterprise applications are available to monitor for critical components without creating new ones from scratch. With McAfee Change Control and McAfee ePO software, new profiles can be activated at any point in time to increase protection—from simple monitoring to bulletproof enforcement.

McAfee ePO software is scalable and readily extensible. It integrates McAfee Change Control software and other McAfee security management products with those of McAfee Security Innovation Alliance Partners. Plus, when McAfee Change Control is teamed with optional change reconciliation software, it provides single-click integration between McAfee ePO software and BMC Remedy.

Enforcement Changes Everything

McAfee Change Control software tracks and validates every attempted change in real time on your server. It enforces change policies by requiring that changes be made within a time window, only by trusted sources, or with approved work tickets. The change prevention component of McAfee Change Control software can be fine-tuned to allow native applications to update their files continuously without interruption, while disallowing all other applications or users from making changes or even reading specified files.

Minimizing Risk and Maximizing Compliance on Multiple Fronts

McAfee offers a wide array of risk and compliance solutions to help you minimize risk, automate compliance, and optimize security. In particular, McAfee Change Control and McAfee Application Control are a powerful combination for eliminating vulnerabilities and ensuring compliance throughout the enterprise.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

41100ds_mcc_1211_fnl_ETMG