Real Time Change Control

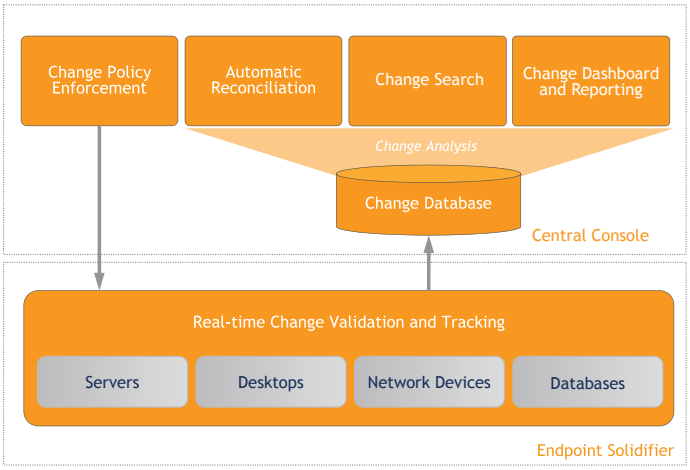
McAfee Change Control

Product overview

Most IT organizations today recognize the centrality of change to their operational effectiveness. Many have invested in process automation tools such as a Change Management system or a Service Desk. Yet, a gap persists between actual change activity and the documented Change Management process. This change control gap results in manual activity by IT departments to control and minimize the costs of change.

McAfee Change Control bridges this gap by adding control to change management. This is accomplished by providing customers with real-time detection of changes being made, accountability to validate change activity and real-time change prevention to block unwanted changes. McAfee Change Control easily automates PCI and SOX controls for compliance reporting, locks down critical systems to ensure only trusted applications run, and prevents change-related outages for improved service availability and accelerated ITIL adoption.

McAfee Change Control is an operational-friendly, low-touch and low overhead software that can be deployed on a wide range of hardware platforms. McAfee Change Control provides change control on servers, network devices (including switches, routers and firewalls), and databases.



Real-Time Change Control

Unlike scan-based solutions which take and compare snapshots of the state of a system, McAfee Change Control continuously tracks and validates every attempted change in real-time. This approach has several important benefits:

- Every change across the infrastructure is recorded in an independent change database the moment it happens
- Every attempted change can be validated in real-time, before the change is applied
- Very little overhead on the endpoint helps eliminate spikes in resource utilization that could interfere with operations.

McAfee's capabilities for capturing all change events across servers, network devices and databases in real-time allows administrators to configure immediate alerts to exceptional changes, which can be fed to the McAfee Change Control dashboard or to an external monitoring application. McAfee Change Control also creates a change database that is comprehensive and always up-to-date. Intelligent filtering ensures that only relevant changes make it to the database, minimizing consumption of network bandwidth. The McAfee change database becomes the foundation for McAfee's powerful search capability, which provides the rich forensic information needed to quickly pinpoint the root-cause of any change-related incident. This capability is also fully-functional when the system in question is offline.

Because every change is captured at the exact moment it occurs, and because it includes rich information about the change, highly accurate reconciliation with change tickets is possible.

McAfee Change Reconciliation, which can operate in concert with McAfee Change Control, correlates the changes made on servers to change tickets documented in existing ticketing systems, and can integrate with popular change management systems such as HP Service Manager and BMC Remedy. McAfee also integrates with popular configuration management databases (CMDB) such as BMC Atrium and HP Universal CMDB.

McAfee Integrity Monitor is designed to help enterprises and service providers quickly, easily and cost-effectively address the database and network device audit trail requirements specified by PCI DSS category 10, as well as the continuous file integrity monitoring requirements specified by PCI DSS category 11. McAfee PCI Pro captures all changes to files, allowing administrators to quickly see where compliance policies are being challenged. The solution identifies and alerts on transient violations, such as when a file is changed inappropriately and then changed back, and also captures specific details about every change including the exact time of the change. In accordance with PCI DSS section 1, McAfee Integrity Monitor also allows organizations to establish configuration standards for network devices and provides the capability to monitor the compliance of the devices in real-time. All configuration changes are tracked and versioned to meet the PCI DSS section 10 requirements for audit trails. Policies can also be set to rollback to a "Trusted Device Configuration" when any unauthorized configuration change is detected. The product provides out-of-the-box PCI reports to demonstrate compliance to auditors with minimal effort, thus reducing the cost of PCI compliance verification.

Finally, the ability to detect and validate attempted changes in real-time enables IT organizations to technically enforce the change policy. The IT organization can now disallow out-of-policy changes attempted on select systems before they occur. This greatly reduces change-related outages and compliance violations.

Enterprise Solutions

Meeting and sustaining PCI DSS compliance

Achieving Payment Card Industry Data Security Standard (PCI DSS) compliance requires merchants and service providers to address approximately 180 individual requirements in 12 categories. However, categories 10 and 11 of the PCI-DSS, which specify the use file integrity monitoring and audit trails, have proven to be the most difficult to fulfill and least satisfied according to recent research. These requirements have been difficult to satisfy because existing tools have merely provided "periodic" file integrity monitoring capabilities that would detect changes through resource-intensive system scans. McAfee Change Control provides categorical control over IT infrastructure, enabling retailers and those who process credit card transactions to fulfill the difficult PCI requirements and validate PCI compliance in an efficient and cost-effective manner.

To help merchants of all sizes easily and cost-effectively address the file integrity monitoring and audit trail requirements outlined in sections 1, 10 and 11 of the PCI DSS, McAfee offers the PCI Pro software. Many of the world's leading qualified security assessors (QSAs) are certifying and recommending these solutions as an essential element of a comprehensive PCI compliance strategy.

Self service Sarbanes-Oxley auditing

The Sarbanes-Oxley Act (SOX), passed by the US Congress in 2002, represents a fundamental shift in corporate governance norms. As corporations come to terms with the implications of SOX to their businesses, one thing is clear: a SOX compliance program is not a one-time project but a sustained effort to gain visibility and accountability into business processes that affect the accuracy of financial reporting. An additional note is that most of the IT controls around SOX compliance are manual, error prone and resource intensive.

McAfee Change Control has helped a number of customers solve their SOX compliance challenges by building a self-service, automated IT control framework in which all the information required to verify compliance is available in a single reporting system - at the click of a button. McAfee's real-time change detection capability along with its automated and highly accurate change reconciliation provides an automated way to validate changes against authorizations. Out-of-process changes (for example, emergency fixes) are automatically documented and reconciled for easier auditability. Customers using McAfee Change Control for Sarbanes-Oxley auditing have realized significant benefits both in terms of reduced risk as well as reduced cost. In most cases, the first phase of benefits comes in the form of automating the existing manual controls. The second phase of benefits comes from rationalizing and reducing the control set, based on demonstrating to auditors that control capabilities are built into the fabric of the environment.

Improve service availability

Most unavailability today is caused by change. IT organizations recognize the centrality of change to their operational effectiveness. The statistics are well-known: 80% of unplanned downtime is caused by unauthorized or untested change. Additionally, 80% of the time taken to restore availability is spent in discovering what changed. Despite this, a gap persists between actual change activity and the documented change process. This change control gap results in manual activity by IT departments to control and minimize the high costs of change and change-related outages.

McAfee Change Control enables IT organizations achieve higher service availability by bridging this change control gap. With McAfee Change Control, changes are tracked in real-time for up-to-the-second change visibility. The rich set of change information McAfee captures is accessible via a powerful and flexible search and reporting interface, dramatically improving forensic ability and speeding diagnostic time. McAfee Change Control enables the selective enforcement of change policies, to prevent unknown changes from occurring before they cause a problem. Customers using McAfee Change Control for continuous service availability have seen dramatic improvements in the number of unavailability incidents (as measured by Mean Time between Failures), as well as recovery time per incident (as measured by Mean Time To Repair). The resulting cost savings, while dependent on the specifics of the environment, is significant.

Accelerate ITIL adoption

Most medium and large-sized organizations are examining ways in which to improve operational efficiency, and ITIL is fast emerging as the de-facto standard in defining a set of best practices around IT operations. The major technical barrier to achieving quick returns on ITIL investments is the lack of control of change across the infrastructure. Without a controlled change environment, all investments in automation and efficiency produce poorer returns than they should because they are essentially operating on a moving target. The major cultural barrier to successful ITIL projects is demonstrating return on investment to the business, particularly since ITIL projects tend to be large, multi-phase implementations.

Customers use McAfee Change Control to dramatically accelerate the pace at which they are able to demonstrate ROI to the business. When McAfee Change Control is deployed, it maintains a controlled environment on which to enable automation. With McAfee Change Control, customers get real-time visibility into change, automated and accurate reconciliation of changes against approvals, and finally, the ability to selectively enforce change policies. They are also able to translate all of this into meaningful returns on investment to the business.

McAfee Change Control Product Specifications

McAfee Change Control Supported Endpoints

Supported Platforms

- Windows XP Professional
- Windows NT Server
- Windows 2000 Server
- Windows 2003 Server
- RedHat Linux 7.2, 8.0 RedHat Enterprise Linux 3.0, 4.0
- Solaris 8, 9, 10
- HP/UX 11.0, 11iV1,11iv2
- AIX 5.3 and 5.2
- IBM iSeries (AS 400)

Supported Databases

- Oracle (7.3, 8.0, 8i, 9i through 10g)
- MS SQL Server (6.5, 7.0, 2000 through 2005)
- Sybase SQL Server (10.X, 11.0, 11.1, 11.5 through 11.9, 12.X)
- IBM DB2 (5.X to 9.X)

Supported Network Devices

- Support for more than 300 devices, including products from Cisco, HP, 3Com, Nortel, Foundry and NetScreen.

Hardware Requirements

- RAM: 256 MB RAM
- Storage: 200MB free disk space

McAfee Change Control Central Console Supported Platforms

Supported Platforms

- Windows 2003 SP1 or higher (NTFS file system)

Hardware Requirements

- CPU: 2.8 Ghz Pentium (Dual CPU recommended)
- RAM: 2048 MB physical RAM (minimum)
- Storage: 80 GB SCSI or Serial ATA hard-disk drives
- Network: 10/100 base T Ethernet

Software Requirements

- Oracle Database Server 9.2 (or greater)
- Internet Explorer 6.0 (or greater) or Firefox 1.0.6 (or greater)

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. www.mcafee.com.

McAfee®

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

6534ds_s3-control-0709_ETMG