Контроль за изменениями в режиме реального времени

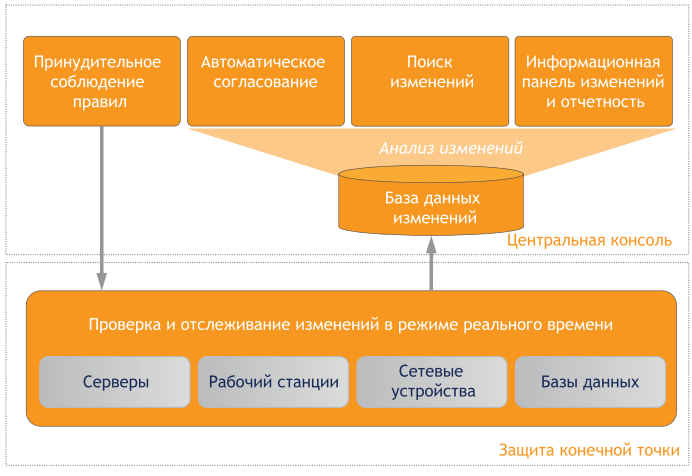
McAfee Change Control

Обзор продукта

Сегодня большинство ИТ-организаций признает важную роль контроля за изменениями для эффективности своей работы. Многие вложили средства в такие инструменты автоматизации технологических процессов, как система управления изменениями или система сервисной поддержки (Service Desk). Тем не менее, существует разрыв между фактическими действиями по внесению изменений и документально оформленным процессом управления изменениями. Этот разрыв в управлении изменениями приводит к необходимости выполнения сотрудниками ИТ-подразделения ручных операций для контроля и минимизации затрат на внесение изменений.

McAfee Change Control устраняет этот разрыв, добавляя к управлению изменениями точный контроль. Это достигается путем предоставления клиентам в режиме реального времени сведений о вносимых изменениях, ведения отчетности для подтверждения их правомерности и предупреждения изменений с целью блокирования нежелательных изменений. McAfee Change Control легко автоматизирует проверку соответствия нормам PCI и SOX для отчетности об их соблюдении, защищает важнейшие системы, позволяя работать только доверенным приложениям, и предотвращает простои, связанные с изменениями, обеспечивая бесперебойную работу и ускоряя внедрение ITIL.

McAfee Change Control – это удобное в эксплуатации и почти не требующее вмешательства программное обеспечение с низким уровнем использования ресурсов, которое можно развертывать на широком спектре аппаратных платформ. McAfee Change Control обеспечивает контроль изменений на серверах, в сетевых устройствах (включая коммутаторы, маршрутизаторы и межсетевые экраны) и базах данных.



Контроль за изменениями в режиме реального времени

В отличие от решений на основе сканирования, которые делают и снимки текущего состояния системы и сопоставляют их, McAfee Change Control непрерывно отслеживает и проверяет каждую попытку внесения изменений в режиме реального времени. Этот подход имеет ряд важных преимуществ:

- Любое изменение в пределах всей инфраструктуры регистрируется в отдельной базе данных изменений в тот момент, когда оно происходит.
- Каждая попытка внесения изменения может проверяться в режиме реального времени, прежде чем изменение будет применено.
- Очень малая дополнительная нагрузка на систему в конечной точке помогает устранить броски в использовании ресурсов, которые могли бы помешать работе.

Возможности McAfee по контролю за всеми событиями изменений на серверах, в сетевых устройствах и базах данных в режиме реального времени позволяют администраторам настроить немедленное оповещение о важных изменениях с подачей сигналов на информационную панель McAfee Change Control или во внешнее приложение мониторинга. McAfee Change Control создает также базу данных изменений, которая носит всеобъемлющий характер и постоянно поддерживается в актуальном состоянии. Интеллектуальная фильтрация гарантирует, что в базу данных вносятся только релевантные изменения, сводя к минимуму потребление ресурсов сети. База данных изменений McAfee становится основой для мощного механизма поиска McAfee, который предоставляет богатую информацию для анализа с целью быстрого определения первопричины любых связанных с изменениями инцидентов. Этот механизм полноценно функционирует и тогда, когда анализируемая система работает в автономном режиме.

Так как каждое изменение фиксируется в тот момент, когда оно происходит, и эта база данных содержит богатую информацию об изменениях, становится возможной высокоточная сверка с запросами на изменения.

Пакет McAfee Change Reconciliation, который может работать совместно с McAfee Change Control, сопоставляет изменения, внесенные на серверах, с картами изменений в существующих системах отслеживания изменений, а также допускает интеграцию с такими популярными системами управления изменениями, как HP Service Manager и BMC Remedy. McAfee можно интегрировать также с популярными базами данных процесса управления конфигурациями (CMDB), такими как BMC Atrium и HP Universal CMDB.

Пакет McAfee Integrity Monitor помогает предприятиям и поставщикам услуг быстро и экономически эффективно выполнять требования по контролю за базами данных и сетевыми устройствами раздела 10 PCI DSS, а также требования по непрерывному контролю целостности файлов раздела 11 PCI DSS. McAfee Pro PCI фиксирует все изменения в файлах, позволяя администраторам быстро определить место возникновения проблем несоблюдения правил. Решение выявляет временные нарушения, например, когда файл был изменен ненадлежащим образом, а затем восстановлен, а также фиксирует конкретные данные о каждом изменении, в том числе его точное время. Кроме того, McAfee Integrity Monitor в соответствии с разделом 1 PCI DSS позволяет организациям создавать стандарты конфигурации для сетевых устройств и обеспечивает возможность контроля в режиме реального времени за соблюдением правил устройствами. Все изменения конфигурации отслеживаются с поддержкой версионности для удовлетворения требований раздела 10 PCI DSS в отношении журналов протоколирования событий. Можно также создавать политики отката к «надежной конфигурации устройства» при обнаружении любого несанкционированного изменения конфигурации. Продукт предоставляет готовые отчеты PCI для подтверждения соответствия аудиторам с минимальными усилиями, тем самым сокращая расходы на проверку соответствия требованиям PCI.

Наконец, способность выявлять и проверять в режиме реального времени попытки внесения изменений позволяет ИТ-организациям технически обеспечить исполнение политики внесения изменений. Теперь ИТ-организация может предупредить попытки внесения изменений вне политики на избранных системах. Это значительно сокращает простои, связанные с изменениями, и количество нарушений.

Характеристики продукта McAfee Change Control

Поддерживаемые конечные точки

Поддерживаемые платформы

- 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)

Поддерживаемые базы данных

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

Поддерживаемые сетевые устройства

- Поддерживает свыше 300 устройств, в том числе продукты Cisco, HP, 3Com, Nortel, Foundry и NetScreen.

Требования к оборудованию

- Оперативная память: 256 МБ
- Внешняя память: 200 МБ свободного дискового пространства

Корпоративные решения

Достижение и поддержание соответствия PCI DSS

Для достижения соответствия Стандарту безопасности данных в индустрии платежных карт (PCI DSS) продавцы товаров и поставщики услуг должны выполнить около 180 отдельных требований по 12 категориям. Причем категории 10 и 11 PCI DSS, которые регламентируют контроль целостности файлов и аудиторские проверки, оказались наиболее трудновыполнимыми, и их, согласно последнему исследованию, соблюдают реже всего. Эти требования было трудно удовлетворить, так как существующие инструменты осуществляли лишь периодические проверки целостности файлов, которые позволяли обнаружить изменения посредством ресурсоемкого сканирования системы. McAfee Change Control обеспечивает полный контроль ИТ-инфраструктуры, позволяя предприятиям розничной торговли и тем, кто обрабатывают транзакции по кредитным картам, выполнить сложные требования PCI и проверять соблюдение PCI эффективным и экономичным способом.

Чтобы помочь торговым предприятиям любых размеров легко и экономически эффективно соблюдать требования контроля целостности файлов и аудита, изложенные в разделах 1,10 и 11 PCI DSS, McAfee предлагает программное обеспечение PCI Pro. Многие ведущие мировые аудиторы по безопасности (Qualified Security Assessor - QSA) сертифицировали и рекомендуют эти решения как важный элемент всеобъемлющей стратегии соответствия стандарту PCI.

Проверка соответствия закону Сарбейнса-Оксли

Закон Сарбейнса-Оксли (SOX), принятый Конгрессом США в 2002 году, привел к фундаментальному сдвигу в нормах корпоративного управления. Когда корпорации столкнулись с последствиями SOX для своего бизнеса, стало ясно: программа соблюдения SOX — это не одноразовый проект, а постоянные усилия по достижению прозрачности и подотчетности бизнес-процессов, которые влияют на точность финансовой отчетности. Следует отметить, что большинство средств ИТ-контроля за соблюдением SOX — это ручные инструменты, чреватые ошибками и интенсивно использующие ресурсы.

McAfee Change Control помог ряду клиентов решить их проблемы соблюдения SOX путем создания самообслуживаемой, автоматизированной системы ИТ-контроля, в которой все сведения, необходимые для проверки соблюдения требований, доступны в единой системе отчетности – одним нажатием кнопки. Возможности McAfee по обнаружению изменений в режиме реального времени в совокупности с автоматизированной и высокоточной системой согласования изменений обеспечивает способ автоматической проверки правомерности изменений. Изменения вне процесса (например, аварийные исправления) автоматически документируются и согласовываются для облегчения ревизии. Клиенты, использующие McAfee Change Control для проверки соответствия закону Сарбейнса-Оксли, осознали значительные выгоды как с точки зрения уменьшения риска, так и снижения расходов. В большинстве случаев на первом этапе выгоды получают в форме автоматизации существующих ручных операций. Затем проявляются выгоды от рационализации и сокращения операций контроля, так как можно продемонстрировать аудиторам, что средства контроля встроены в структуру самой среды.

Обеспечение непрерывности бизнеса

Сегодня большинство простоев вызвано изменениями. ИТ-организации признают центральную роль изменений для эффективности своей работы. Статистика хорошо известна: 80% внеплановых простоев вызвано несанкционированными или непроверенными изменениями. Кроме того, 80% времени, затрачиваемого на восстановление работоспособности, расходуется на определение того, что именно изменилось. Тем не менее, разрыв между фактическими действиями по внесению изменений и документально оформленным процессом управления изменениями сохраняется. Этот разрыв в управлении изменениями приводит к ручным операциям по контролю и минимизации изменений и связанных с ними дорогостоящих простоев.

McAfee

Характеристики продукта McAfee Change Control

Центральная консоль McAfee Change Control

Поддерживаемые платформы

- Windows 2003 SP1 или более поздняя версия (файловая система NTFS)

Требования к оборудованию

- Процессор: Pentium 2,8 ГГц (рекомендуется двухпроцессорная конфигурация)
- Оперативная память: 2048 МБ физической памяти (минимум)
- Внешняя память: жесткие диски SCSI или Serial ATA емкостью 80 ГБ
- Сеть: Ethernet baseT 10/100 Гбит/с

Требования к программному обеспечению

- Oracle Database Server 9.2 (или более поздняя версия)
- Internet Explorer 6.0 (или более поздняя версия) or Firefox 1.0.6 (или более поздняя версия)

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

McAfee Change Control позволяет ИТ-организациям достичь более высокой доступности услуг путем устранения этого разрыва в контроле за изменениями. Благодаря McAfee Change Control, изменения отслеживаются в режиме реального времени с точностью до секунды. Богатая информация об изменениях, которую собирает McAfee, предоставляется через мощный и гибкий интерфейс поиска и отчетности, который значительно упрощает экспертизу и ускоряет диагностику. McAfee Change Control позволяет избирательно применять политику изменений, предотвращая проблемы, вызванные бесконтрольным внесением изменений. Клиенты, использующие McAfee Change Control для достижения бесперебойной работы, добиваются значительного уменьшения числа инцидентов (среднее время бесперебойной работы) и времени восстановления на инцидент (среднее время восстановления). В результате достигается ощутимая, хотя и зависящая от особенностей среды, экономия.

Ускорение освоения ITIL

Большинство средних и крупных организаций изучают возможности для повышения эффективности работы, и библиотека передового ИТ-опыта ITIL быстро становится стандартом де-факто для определения набора передовых методов работы ИТ-подразделения. Главным техническим препятствием для достижения быстрой отдачи от инвестиций в ITIL является отсутствие контроля за изменениями по всей инфраструктуре. Без среды с контролируемыми изменениями все инвестиции в автоматизацию и повышение эффективности производства приносят недостаточные результаты, поскольку это, по существу, стрельба по движущейся мишени. Главное психологическое препятствие для успешных проектов ITIL — это трудность демонстрации окупаемости инвестиций, особенно для крупных и многоэтапных ITIL-проектов.

Заказчики используют McAfee Change Control, чтобы значительно приблизить момент, когда можно наглядно продемонстрировать окупаемость инвестиций. После установки программное обеспечение McAfee Change Control поддерживает контролируемую среду, допускающую автоматизацию. Благодаря McAfee Change Control заказчики получают информацию об изменениях в режиме реального времени, автоматическое и точное согласование изменений в процессе их утверждения и, наконец, возможность выборочного соблюдения политики изменений. Все это они могут перевести в ощутимую отдачу от инвестиций.

О компании McAfee

Корпорация McAfee, штаб-квартира которой расположена в г.Санта-Клара (штат Калифорния, США), является ведущим поставщиком решений в области информационной безопасности. McAfee неустанно решает самые сложные в мире задачи в области безопасности. Компания предлагает действенные и проверенные решения и услуги, которые помогают защитить системы и сети по всему миру, позволяя заказчикам безопасно подключаться к интернету, просматривать информацию и делать покупки. Отмеченный наградами коллектив инженеров McAfee создает инновационные продукты, которые служат потребителям, предприятиям, государственным организациям и поставщикам услуг, позволяя им соблюдать установленные стандарты и нормы, защищать свои данные, предотвращать сетевые вторжения, выявлять уязвимости и постоянно контролировать и повышать безопасность своих систем. www.mcafee.com

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