McAfee Integrity Monitor

Контроль целостности файлов в режиме реального времени

Для соблюдения строгих нормативных требований в ИТ-инфраструктуре необходимы два основных компонента: уверенность в состоянии системы и возможность проверки и внесения санкционированных изменений без нарушения корпоративных стандартов и государственных нормативных актов. В частности, необходимость обеспечения безопасного внесения изменений подчеркивается в разделах 10.5.5 («Следует использовать приложения контроля целостности файлов для защиты журналов протоколирования событий от несанкционированных изменений») и 11.5 («Следует использовать приложения контроля целостности файлов для оповещения персонала о несанкционированных изменениях критичных системных файлов и файлов данных») Стандарта безопасности данных индустрии платежных карт (PCI DSS).

Независимое исследование показало, что контроль целостности файлов относится к числу наименее соблюдаемых из всех нормативных требований: его не выполняют почти в 40% случаев несоблюдения PCI. Хотя многие ИТ-организации, вынужденные соблюдать PCI и другие положения, смотрят в сторону решений для контроля целостности файлов (File Integrity Monitoring – FIM), каждый, кто оценивает эти решения, должен учитывать, что технология в этой области значительно изменилась, и появилось новое поколение решений.

FIM — это возможность контролировать файлы и каталоги на сервере на наличие изменений в содержании, в правах доступа или же изменений обоих типов. McAfee® Integrity Monitor обеспечивает контроль целостности файлов в режиме реального времени, выходя за рамки распространенных сегодня решений для контроля целостности файлов, действующих по принципу «периодического» мониторинга, то есть решений на основе сканирования. Это более эффективное решение от McAfee снижает риск, устраняя разрыв во времени и исключает нагрузку, характерную для мониторинга на основе сканирования. Оно гарантирует соблюдение требования стандарта PCI DSS, предписывающего тестировать и проверять безопасность вычислительной среды.

Основные преимущества

- Отображение изменений в распределенных системах, таких как инфраструктуры торговых терминалов и центров обработки данных
- Централизованные отчеты о состоянии систем и сигнализация об изменениях в стандартных ИТ-инфраструктурах
- Контроль целостности файлов в соответствии с требованиями PCI DSS для неоднородных систем

Сравнение FIM реального времени и периодического FIM

Существуют два подхода к контролю целостности файлов: периодический мониторинг и мониторинг реального времени.

- *Периодический мониторинг* — Традиционные решения мониторинга от большинства других производителей можно охарактеризовать как решения для мониторинга целостности файлов периодического действия. Они обнаруживают изменения в файлах путем проведения периодических сканирований системы и сравнения результатов, выявляя изменения, внесенные в промежутке между сканированиями, и сообщая о любых таких изменениях. При этом изменения, внесенные во время самого процесса сканирования, не обнаруживаются.
- *FIM реального времени* — Это новейшая технология мониторинга, которая постоянно отслеживает файлы. Изменения обнаруживаются в тот момент, когда они происходят, и о любых нарушениях немедленно сообщается.

Преимущества FIM реального времени от McAfee

- *Полное обнаружение изменений* – McAfee Integrity Monitor фиксирует каждое изменение в файле. Периодические FIM пропустили бы изменения, которые в промежутке между сканированиями происходили неоднократно. Обнаружение всех изменений имеет важное значение для поддержания соответствия, поскольку позволяет организациям выявить проблемы несоблюдения правил и устранить неправомерные изменения в их источнике.

Выявление временных нарушений – Если файл был изменен ненадлежащим образом, а затем возвращен в первоначальное состояние, имеет место временное нарушение. Периодические решения FIM неспособны обнаружить такие нарушения. Так как McAfee Integrity Monitor фиксирует все изменения, он подаст сигнал и в случае временного нарушения, даже если оно было быстро устранено.

- *Сбор данных для экспертизы* – FIM реального времени McAfee Integrity Monitor регистрирует всю информацию о любом изменении, в том числе точное время изменения, кто был зарегистрирован в машине на тот момент, какие процессы (например, редакторы) в это время работали; вносились ли изменения вручную или с помощью разрешенной программы, и если они вносились вручную, то каким пользователем. Эта информация имеет решающее значение для выявления различий между безопасным, санкционированным изменением и нарушением. Она позволяет также быстро провести расследование проблем, вызванных изменением. Продукты FIM периодического действия не отражают эту важнейшую информацию.
- *Отсутствие компромиссов* – Сканирование всей системы может оказаться дорогостоящим и ресурсоемким делом, поэтому периодические решения FIM оптимизируют процесс сканирования, разыскивая изменения только в определенных файлах. При таком подходе можно пропустить неизвестные изменения (например, если обновление содержит новый файл или каталог, еще не внесенный в список сканирования). FIM реального времени McAfee Integrity Monitor чрезвычайно мало нагружает ресурсы системы, так что можно контролировать всю инфраструктуру, не оказывая влияния на ее работу.

Мониторинг защищенной среды

McAfee Integrity Monitoring обеспечивает соблюдение нормативных требований и сигнализацию об изменениях не только для серверов, но и охватывает другие компоненты, такие как базы данных и сети, создавая единое представление для отчетности об изменениях и сигнализируя об изменениях во всей ИТ-среде предприятия. Широкий спектр платформ, поддерживаемых McAfee Integrity Monitoring, завершают альтернативные компоненты, такие как виртуальные серверы, POS-терминалы на базе ОС IBM4690 и системы IBM AS400, обычно не охватываемые другими поставщиками FIM.

- *Мониторинг баз данных* – контролирует три ключевых области:
  - Действия (вход, выход, создание пользователей / ролей, смена пароля и т.д.)
  - Изменения схемы (создание/редактирование таблиц, индексы, хранимые процедуры и т.д.)
  - Изменение данных (вставка/редактирование/удаление конфиденциальных записей)
- *Мониторинг конфигурации сети* – Сигнализирует об изменении конфигурации наиболее часто используемых сетевых компонентов.

- *AS400* – Контроль в режиме реального времени целостности этой распространенной корпоративной платформы повышает ее ценность и обеспечивает соблюдение нормативных требований в этой мощной инфраструктуре
- *IBM4690* – Преобладающая платформа POS-терминалов получила решение для контроля целостности файлов, предоставляющее предприятиям розничной торговли расширенные возможности по поддержанию соответствия требованиям PCI

Узнайте новое о своем предприятии

McAfee Integrity Monitor помогает ИТ-менеджерам, директорам и руководителям ИТ-подразделений получать информацию реального времени и отчеты, которые позволяют им узнать нечто новое о своем предприятии. Возможности для выявления изменений в распределенных системах торговой сети или инфраструктурах центров обработки данных позволяют ИТ-персоналу обеспечить приоритет санкционированных изменений перед несанкционированными или потенциально злонамеренными действиями.

McAfee Integrity Monitor дает представление о фактической деятельности и изменениях, которые вносятся в эту критическую инфраструктуру, и гарантирует непрерывность бизнеса.

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

6915brf_dtp_integrity-monitoring_0809_ETMG