McAfee Enterprise Log Manager

Снижение расходов на обеспечение нормативно-правового соответствия благодаря автоматизации сбора, хранения и обработки журналов

Правильный сбор и хранение журналов позволит вам сократить расходы на обеспечение нормативно-правового соответствия и создать четкий аудиторский (контрольный) след, который невозможно оспорить. McAfee® Enterprise Log Manager представляет собой эффективное средство сбора, сжатия и хранения всех файлов журналов. Интеграция с McAfee Enterprise Security Manager позволяет использовать расширенные функции поиска, анализа и сопоставления данных, оповещения о событиях и формирования отчетов. Все события и оповещения дают возможность одним щелчком мыши получить доступ к исходной записи системного журнала, что упрощает работу по проведению компьютерно-технических экспертиз.

Ключевые преимущества

- Универсальный сбор и хранение журналов для обеспечения нормативно-правового соответствия
- Гибкая настройка места и условий хранения для каждого источника журналов
- Поддержка сохранности вещественных доказательств и компьютерно-технических экспертиз
- Анализ журналов и поиск по журналам
- Журналы хранятся локально или в управляемой сети SAN
- Полная интеграция с McAfee Enterprise Security Manager
- Имеются смешанные варианты поставки, подразумевающие использование физических и виртуальных устройств

Решение McAfee Enterprise Log Manager предназначено для сбора, подписи и хранения файлов журналов. Оно автоматизирует процессы обработки и анализа журналов всех типов, включая журналы событий Microsoft Windows, журналы баз данных, журналы приложений и системные журналы. Журналы подписываются и утверждаются, что обеспечивает их аутентичность и целостность в соответствии с нормативно-правовыми требованиями. Наличие готовых к использованию наборов правил и отчетов упрощает процесс предоставления доказательств нормативно-правового соответствия и применения политик в вашей организации.

Использование этого комплексного решения для сбора, обработки и анализа журналов повысит ваш уровень безопасности и даст вам возможность значительно легче обеспечивать соответствие таким стандартам, как PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA и SOX.

Интеллектуальное управление журналами

McAfee Enterprise Log Manager осуществляет интеллектуальный сбор журналов: журналы, необходимые для обеспечения нормативно-правового соответствия, он сохраняет, а журналы, необходимые для обеспечения безопасности, он обрабатывает и анализирует. Он позволяет хранить журналы в исходном формате столько времени, сколько потребуется для выполнения тех или иных задач по обеспечению нормативно-правового соответствия. Поскольку McAfee не вносит изменений в исходные файлы журналов, данное решение поддерживает функции обеспечения сохранности вещественных доказательств и невозможности отказа от них.

Потребности в хранении информации различаются в зависимости от источника журналов и подлежащих выполнению требований нормативно-правового соответствия. McAfee Enterprise Log Manager использует легко настраиваемые пулы хранения, которые позволяют обеспечить правильное хранение ваших журналов в течение необходимого времени. Выберите наилучший вариант хранения, отвечающий вашим потребностям: на жестком диске, установленном в устройстве, или в высокоскоростной сети SAN с использованием дополнительных оптоволоконных карт.

Впрочем, одних только файлов журналов недостаточно для получения всей необходимой информации. Файлы журналов содержат важные факты и являются существенным звеном в выстраивании цепочки сохранения вещественных доказательств, однако они не отвечают на вопросы, важные с точки зрения безопасности. Так, например, в журнале доступа может быть сохранено имя пользователя, а информации о роли и правах этого пользователя может не быть. В журнале может быть указано, к какой системе был осуществлен доступ, но не быть никаких данных о том, какие типы данных используются в этой системе и кто должен получать доступ к этим данным.

intel Security

Интеграция с McAfee Enterprise Security Manager

Решение McAfee Enterprise Log Manager является дополнительным встраиваемым компонентом McAfee Enterprise Security Manager. Если McAfee Enterprise Log Manager служит для хранения журналов, то McAfee Enterprise Security Manager осуществляет комплексный разбор, нормализацию и анализ журналов, благодаря чему данные журналов становятся немедленно доступными для проведения расследований событий системы безопасности и реагирования на инциденты в режиме реального времени.

При создании события безопасности проанализированные файлы события привязываются непосредственно к исходному файлу журнала и к конкретной записи журнала, что позволяет получать к ним доступ одним щелчком мыши. Это облегчает процессы управления событиями и проведения компьютерно-технических экспертиз, поскольку избавляет администраторов от необходимости осуществления дополнительных действий, запуска дополнительных приложений или трудоемкого поиска данных вручную.

Насыщенный контекст для анализа

Совместное использование McAfee Enterprise Security Manager и McAfee Enterprise Log Manager позволяет получить контекст для каждого журнала, поэтому все проанализированные записи журналов приобретают особую ценность. Контекстная информация может быть следующая:

- IP-адрес источника или пункта назначения;
- идентификационная информация;
- имя узла или службы, к которым был осуществлен доступ;
- данные об уязвимости, полученные от анализатора уязвимости;
- данные о топологии сети;
- данные о политике и конфиденциальности.

Гибкие пулы хранения

Используемые в McAfee Enterprise Log Manager пулы хранения позволяют сделать процесс долгосрочного хранения журналов более гибким. Пулы хранения представляют собой виртуальные группы доступного пространства, которые могут распределяться между различными группами физических устройств хранения данных (локальные накопители, NFS, SAN, CIF и т. д.) для удовлетворения разных требований по управлению журналами.

Рис. 1. Гибкие пулы хранения поддерживают настраиваемые сроки хранения журналов.

Пул хранения может состоять из нескольких разных устройств, а данные можно размещать в том или ином пуле в зависимости от исходного устройства. Это позволяет хранить разные журналы в разных местах исходя из степени их важности с точки зрения обеспечения безопасности, нормативно-правового соответствия, конфиденциальности и проч. Например, журналы, критически важные для обеспечения нормативно-правового соответствия, можно хранить в пуле, состоящем из нескольких разных устройств хранения с сетевым резервированием. Менее важные журналы можно хранить в системах с меньшей степенью резервирования. А журналы, необходимые для проведения компьютерно-технических экспертиз, можно хранить на локальном накопителе, который позволяет выполнять быстрый анализ событий.

Быстрое развертывание

McAfee Enterprise Log Manager и McAfee Enterprise Security Manager можно развернуть совместно с помощью единого комбинированного устройства, либо распределить по сети, что позволяет обеспечить поддержку даже самых крупных корпоративных сетей. Имеются также смешанные варианты поставки, подразумевающие использование физических и виртуальных устройств.

Интеграция в вашу инфраструктуру

Если большинство решений для управления журналами работает автономно, то McAfee Enterprise Log Manager взаимодействует с другими системами обеспечения информационной безопасности. Подключаясь к вашей инфраструктуре безопасности через McAfee Enterprise Security Manager, он упрощает операции по обеспечению безопасности, повышает общий уровень эффективности и снижает расходы. Вы получаете возможность интегрировать функции интеллектуального управления журналами с мощными функциями анализа, проверки сети, мониторинга событий баз данных и др.

За дополнительной информацией обращайтесь по адресу **www.mcafee.com/ru/products/siem/index.aspx**.

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com