McAfee Enterprise Security Manager

Обнаружение. Реагирование. Соответствие.

Самая эффективная защита начинается с получения точной картины всего происходящего в системах, сетях, базах данных и приложениях в режиме реального времени. McAfee® Enterprise Security Manager — основное решение в семействе систем управления информацией о безопасности и событиями безопасности (SIEM) от компании McAfee — отличается высокой производительностью, предоставляет информацию для принятия необходимых мер и обеспечивает осведомленность о ситуации в режиме реального времени. Быстродействие и масштаб этого решения позволяют специалистам по безопасности выявлять, анализировать и обезвреживать скрытые угрозы, в то время как встроенная структура обеспечения нормативно-правового соответствия упрощает контроль за соблюдением требований.

Ключевые преимущества

- Представление оперативных и архивных данных для комплексного обнаружения и устранения угроз
- Предоставление информации, имеющей практическую ценность для быстрого реагирования на приоритетные угрозы
- Передовые средства анализа и обогащения данных для преобразования данных в информацию о безопасности
- Структура нормативно-правового соответствия для более чем 240 мировых стандартов

McAfee Enterprise Security Manager помогает разобраться в поступающей в режиме реального времени информации об окружающем мире — в том числе об угрозах, репутации и уязвимостях, — а также обеспечивает представление сведений о системах, данных, рисках и действиях внутри компании. В результате ваши ИТ-специалисты получают долгожданную возможность полного доступа к содержимому и контекстной информации, сопоставление которых необходимо для анализа рисков и быстрого принятия решений, чтобы использовать ресурсы с максимальной эффективностью в условиях быстро меняющихся угроз безопасности. Это является важной предпосылкой для успешного расследования атак, имеющих затяжной и скрытый характер, для поиска признаков взлома или для устранения несоответствий нормативно-правовым требованиям.
Для оптимизации эффективности операций по обеспечению безопасности в McAfee Enterprise Security Manager также интегрированы инструменты для управления конфигурациями и изменениями, управления ситуациями и централизованного управления политиками — всё, что необходимо для оптимизации рабочих процессов и облегчения повседневных действий по обеспечению информационной безопасности.

Передовая система сбора информации об угрозах

Любое отклонение от нормы, обнаруженное в сетевом трафике, действиях пользователей или поведении приложений может свидетельствовать о наличии угрозы и о том, что ваши данные или ваша инфраструктура подвержены риску. McAfee Enterprise Security Manager в режиме реального времени рассчитывает базовый уровень активности для всей собираемой информации.
Это решение заблаговременно создает уведомления о потенциальных угрозах с учетом их приоритета и параллельно анализирует собранные данные на наличие признаков более крупных угроз. Кроме того, чтобы облегчить понимание взаимосвязи событий безопасности с реальными бизнес-процессами, McAfee Enterprise Security Manager снабжает каждое событие контекстной информацией (полученной, например, от средств поиска уязвимостей и систем управления персональными

intel Security

Возможность выполнять масштабируемое развертывание

- Смешанные варианты поставки включают в себя физические и виртуальные устройства с возможностью обеспечения высокой доступности.
- Развертывание на одном устройстве для небольших компаний или распределенные решения для крупных предприятий.
- Высокомасштабируемые устройства обеспечивают сбор больших объемов данных из разнообразных источников в системах защиты и инфраструктуре организации.

и учетными данными). Такая информация помогает организациям предоставлять необходимые данные соответствующим специалистам для принятия оперативных мер и рациональных решений.

Сбор критически важных фактов за минуты, а не за часы

Наше высокопроизводительное аппаратное устройство для работы с базами данных может собирать и обрабатывать миллиарды журнальных событий, накопленных на протяжении многих лет, и сопоставлять их с другими потоками данных на скорости, отвечающей потребностям крупных предприятий. McAfee Enterprise Security Manager в состоянии хранить миллиарды событий и потоков данных, обеспечивая непрерывную доступность всей информации для спонтанных запросов, проведения компьютерно-технических экспертиз, проверки правил и обеспечения нормативно-правового соответствия.

Возможность быстрого доступа к устройствам долгосрочного хранения данных о событиях является важной предпосылкой для успешного расследования атак, имеющих затяжной и скрытый характер, для поиска признаков постоянных угроз повышенной сложности (advanced persistent threats — APT) и для исправления ошибок, обнаруживаемых в ходе аудитов нормативно-правового соответствия — для всего этого требуется полный доступ ко всей информации по каждому конкретному событию и возможность анализа архивных данных.

Предназначено для обеспечения безопасности при работе с «большими данными»

Безопасность больших объемов неопределенно структурированных данных («больших данных») может иметь чрезвычайно важное значение. Постоянно растущие объемы информации, в частности о событиях, активах, угрозах и пользователях, создают значительные трудности для отделов безопасности. Для преодоления этих трудностей в McAfee Enterprise Security Manager реализована система управления данными, специально предназначенная для выполнения операций, необходимых решению SIEM. По мнению компании Gartner, эта система управления данными относится к основным преимуществам решений SIEM компании McAfee.

Решение McAfee Enterprise Security Manager обеспечивает хранение огромных объемов контекстных данных (сотен миллионов точек) и дополнение событий контекстной информацией в режиме реального времени. Вся эти данные тщательным образом индексированы, нормализованы и сопоставлены между собой с целью обнаружения большего количества рисков и угроз безопасности. McAfee Enterprise Security Manager быстро реагирует как на простые, так и на сложные запросы. Эффективная система индексирования позволяет решению выполнять параллельные операции с оперативными и архивными данными для оптимизации анализа угроз и компьютерно-технических экспертиз. Ключевым требованием к SIEM является интеллектуальный анализ больших объемов неопределенно структурированных данных для нахождения критически важной информации о безопасности. McAfee Enterprise Security Manager эффективно использует большие объемы данных о безопасности, не ограничиваясь простым сопоставлением образцов. Это решение обнаруживает долгосрочные признаки взлома и предоставляет информацию об угрозах, имеющую практическую ценность.

Анализ контекста и содержимого

Наличие контекстной информации (собираемой с помощью средств поиска уязвимостей, систем управления персональными и учетными данными, решений для обеспечения конфиденциальности данных и других поддерживаемых систем) позволяет снабжать каждое событие контекстом, облегчающим понимание того, как сетевые события и события в системе безопасности соотносятся с реальными бизнес-процессами и политиками.

Благодаря масштабируемости и быстродействию McAfee Enterprise Security Manager позволяет собирать большее количество информации из большего количества источников (включая используемые в разных приложениях данные, такие как документы, транзакции и сообщения), что значительно облегчает проведение компьютерно-технических экспертиз. Вся эти данные тщательно индексируются, нормализуются и сопоставляются между собой с целью обнаружения большего количества рисков и угроз безопасности.

Оптимизация операций по обеспечению безопасности

Чтобы оптимизировать операции по обеспечению безопасности, McAfee Enterprise Security Manager представляет в одном окне целостную картину уровня защищенности предприятия, состояния нормативно-правового соответствия и приоритетных проблем безопасности, требующих расследования.

McAfee Enterprise Security Manager обеспечивает удобство в использовании без дополнительных усилий: в распоряжении специалистов оказываются сотни отчетов, представлений, правил и предупреждений, которые можно легко настраивать. Например, пользователи панели мониторинга McAfee Enterprise Security Manager могут настроить базовый уровень для оценки типичного использования сети или задать индивидуальные параметры предупреждений. Эта панель позволяет легко визуализировать важнейшие сведения о безопасности, исследовать их и составлять отчеты на их основе. В результате организации получают долгожданную возможность полного доступа к содержимому и контекстным данным, сопоставление которых необходимо для принятия быстрых и рациональных решений.

Упрощение процесса обеспечения нормативно-правового соответствия

Благодаря централизации и автоматизации мониторинга нормативно-правового соответствия и формирования соответствующих отчетов McAfee Enterprise Security Manager позволяет отказаться от трудоемких ручных процессов. Кроме того, интеграция с Unified Compliance Framework (UCF) дает возможность применить методику однократного сбора данных для соблюдения многочисленных требований, что сводит к минимуму трудовые и финансовые затраты на проведение аудита. Поддержка UCF повышает эффективность процесса обеспечения нормативно-правового соответствия путем нормализации требований всех стандартов, что позволяет легко сопоставлять единый набор сведений о событиях с множеством отдельных нормативов.

Для упрощения и ускорения процесса управления обеспечением нормативно-правового соответствия McAfee Enterprise Security Manager включает в себя сотни готовых панелей мониторинга, всеобъемлющие журналы аудита и отчеты, отвечающие требованиям более чем 240 мировых стандартов и регламентирующих систем, в том числе PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX и SOX. Помимо обширных встроенных возможностей, все отчеты, правила и панели мониторинга McAfee Enterprise Security Manager поддерживают полную индивидуальную настройку.

Объединение вашей ИТ-инфраструктуры

Интеграция решений для обеспечения безопасности и нормативно-правового соответствия обеспечивает больше преимуществ, чем использование их по отдельности, и позволяет получать беспрецедентно подробную информацию об уровне защищенности предприятия в режиме реального времени. Решения SIEM от компании McAfee собирают ценные данные с сотен типов защитных устройств в инфраструктуре предприятия. Помимо этого, McAfee Enterprise Security Manager поддерживает активную интеграцию с платформой McAfee® ePolicy Orchestrator® (McAfee ePO™) для управления конечными точками на основе политик, с решением McAfee Network Security Manager для предотвращения вторжений и с решением McAfee Vulnerability Manager для поиска и устранения уязвимостей.

McAfee Enterprise Security Manager интегрирован с McAfee Threat Intelligence Exchange. В отличие от стандартных подходов к обеспечению безопасности, это сочетание позволяет организациям использовать преимущества замкнутого рабочего процесса, охватывающего все этапы от обнаружения до нейтрализации угроз. На основании мониторинга конечных точек McAfee Threat Intelligence Exchange собирает сведения о малораспространенных атаках, используя при этом глобальные, сторонние и локальные данные об угрозах. Кроме того, для дальнейшего анализа и классификации файлов McAfee Threat Intelligence Exchange может использовать любой продукт, интегрированный с платформой Security

Connected, например McAfee Advanced Threat Defense. Такой подход обеспечивает для организаций осведомленность о ситуации и контексте, позволяя оценить воздействие событий безопасности на реальные бизнес-процессы и политики и сосредоточить усилия службы безопасности на самых важных проблемах.

Столь глубокая интеграция защитных решений McAfee поднимает осведомленность о безопасности на новый уровень, при котором управлять защитными действиями можно из консоли McAfee Enterprise Security Manager. McAfee Enterprise Security Manager использует преимущества интеграции для смены политик на конечных точках, помещения подозрительных систем в карантин, а также сбора важнейших сведений путем поиска уязвимостей. Опять же, все эти действия выполняются из консоли McAfee Enterprise Security Manager. Интеграция McAfee Global Threat Intelligence (McAfee GTI) с McAfee Enterprise Security Manager позволяет получать данные от более чем 100 миллионов глобальных датчиков угроз McAfee Labs в виде постоянно обновляемого потока известных вредоносных IP-адресов. Благодаря такой интеграции McAfee Enterprise Security Manager может автоматизировать многие меры первоочередного реагирования, что помогает организациям повысить быстроту и эффективность реагирования на атаки.

Платформа Security Connected компании McAfee обеспечивает единую структуру, в рамках которой сотни продуктов, служб и партнеров могут взаимодействовать между собой. Используя решения Security Connected, такие как McAfee Enterprise Security Manager, специалисты по безопасности могут просматривать контекстные данные в режиме реального времени, мгновенно получая представление об уровне защищенности предприятия в масштабе всей инфраструктуры. Это позволяет организациям минимизировать время, затрачиваемое на нейтрализацию угроз после их обнаружения.

Дополнительная информация

Дополнительную информацию о McAfee Enterprise Security Manager можно получить 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