McAfee Content Security Reporter

Анализ. Действие. Применение.

Сложность нередко выступает врагом информационной безопасности, хотя сами информационные технологии сегодня намного сложнее, чем прежде. Так, например, мобильные устройства и тенденция ориентирования ИТ на потребителя порождают множество угроз привычным методам управления защитой предприятия. Децентрализация информационных технологий, обусловленная ростом зависимости от ресурсов третьих сторон, а также такие модели, как облачные вычисления или программное обеспечение как услуга (Software-as-a-Service, SaaS) порождают новые проблемы управления, в то время как растущая сложность атак предъявляет все более высокие требования к системам защиты.

Чтобы справиться с такими сложными задачами, администраторам систем безопасности следует унифицировать и упрощать свою тактику работы. Это позволит им более оптимально использовать ограниченные ресурсы. Им необходимы автоматизированные и взаимосвязанные продукты для обеспечения безопасности, которые, взаимодействуя между собой, обеспечат:

- ситуационную осведомленность обо всех продуктах и направлениях угроз, необходимую для поддержки точного и оперативного анализа угроз;
- централизованное управление и контроль для достижения максимальной эффективности действий;
- простые процессы, способствующие эффективному применению корпоративной политики безопасности.

Решение McAfee® Content Security Reporter связывает подробный анализ с возможностями принятия эффективных действий и положительной реализацией целей защиты. Система представляет подробные сведения обо всех наиболее актуальных направлениях угроз и о вредоносном содержимом, цель которых — проникнуть сквозь защиту периметра через сеть, электронную почту и веб-трафик.

McAfee Content Security Reporter объединяет анализ данных и меры, обеспечиваемые решениями для предотвращения вторжений в сеть, а также технологиями защиты электронной почты и веб-трафика. Средства анализа встроены непосредственно в программное обеспечение ePolicy Orchestrator™ (McAfee ePO™) и тем самым расширяют возможности единой панели управления, которая сводит воедино данные о всем спектре угроз информационной безопасности. Система предоставляет администраторам большой и гибкий

Поддерживаемые источники данных

- McAfee Web Gateway
- McAfee SaaS Web Protection
- McAfee Firewall Enterprise
- McAfee Email Gateway и McAfee SaaS Email Protection and Continuity
- McAfee Network Security Platform
- McAfee SmartFilter (только протокол фильтрации интернет-трафика)

Развертывание

Программное обеспечение (Windows Server; требуется McAfee ePO 4.6.5 или выше)

набор инструментов, позволяющих лучше понимать угрозы, исходящие от сетевого содержимого, сопоставлять детальные сведения с предпринимаемыми действиями, используя рабочие процессы, усиливающие защиту в стратегических точках управления на основе анализа содержимого.

Анализ

McAfee Content Security Reporter автоматически импортирует из поддерживаемых сетевых продуктов McAfee широкий спектр данных о веб-защите, защите электронной почты и предотвращении вторжений в сеть.

Аналитические отчеты McAfee Web Protection включают:

- анализ тенденций использования Интернета, которые можно фильтровать с помощью программного обеспечения как услуги (SaaS) или шлюза;
- функции веб-защиты для защиты от вредоносных программ и применения политик фильтрации;
- сводки о применении политик веб-защиты в отношении разрешенных и заблокированных взаимодействий;
- основные веб-пользователи;
- основные IP-адреса веб-клиентов;
- основные категории риска безопасности;
- обнаруженные вредоносные программы по веб-сайтам;
- основные конечные точки с обнаруженными вредоносными программами;
- подробные сведения обо всех точках данных, включая пользователя, действие, предпринятое исходя из политики, браузер, IP-адрес сети и исходные данные.

Решение McAfee Email Protection осуществляет анализ угроз, связанных с обменом сообщениями, в том числе проверяя:

- доставленные, принятые и отклоненные сообщения электронной почты, которые в случае гибридной архитектуры могут быть отфильтрованы по формфактору;
- сообщения, не удовлетворяющие требованиям стандартов электронной почты;
- попытки фишинга и нежелательные сообщения;
- отклоненные сообщения;
- несоответствующее или вредоносное содержимое;
- сводка об электронной почте по обнаруженным угрозам (вирусы, фишинг, нежелательная почта, несоответствие требованиям) и методам обнаружения (предотвращение утечек данных, фильтр содержимого, анализ изображений, размер сообщений и др.);
- основных внутренних отправителей и получателей заблокированных или контролируемых сообщений электронной почты.

Данные McAfee Network Security Platform включают подробное описание обнаруженных в содержимом сети угроз, в том числе:

- определенные типы атак, включая основные атаки по частоте, источнику и адресу назначения;
- сводку об атаках по категориям;
- сводку об атаках по степени опасности;
- сводку об атаках по отправителям;
- подробные сведения, такие как имя датчика, дата/время, категория атаки.

Действие

McAfee Content Security Reporter позволяет группам обеспечения безопасности применять к данным о защите содержимого широкий спектр аналитических методов в сочетании с аналитическими возможностями и средствами, реализованными в программном обеспечении McAfee ePO. Аналитические методы включают:

- одновременное отображение нескольких представлений данных McAfee Content Security Reporter по различным запросам на панелях мониторинга McAfee ePO;

- панели мониторинга и фильтры отчетов, которые обособляют конкретные данные и могут настраиваться для выполнения конкретных видов анализа;
- доступ к дополнительной информации об угрозах, получаемой с помощью технологии McAfee Global Threat Intelligence (McAfee GTI);
- открытие и проверку веб-сайтов непосредственно по URL-адресам, выделенным в панелях мониторинга решения McAfee Content Security Reporter.

Применение

McAfee® Content Security Reporter связывает данные анализа с действиями по применению политик безопасности, включая:

- интеграцию с общим каталогом решения McAfee ePO, позволяющую администраторам устанавливать те или иные действия по применению политик безопасности;
- добавление в список для блокирования или разрешения непосредственно из представлений панели мониторинга;
- средства управления на основе ролей с поддержкой разделения полномочий при доступе к данным и управлении политиками безопасности.

Организации не могут себе позволить иметь участки, не защищенные от угроз со стороны сетей, электронной почты и веб-содержимого. McAfee Content Security Reporter ликвидирует эту брешь в защите благодаря аналитическим возможностям, расширяющим интегрированные методы анализа, имеющиеся в программном обеспечении. Ключевые преимущества включают интеграцию с программным обеспечением McAfee ePO, возможность сбора подробных сведений непосредственно из поддерживаемых систем безопасности и возможность принимать меры реагирования непосредственно в отношении сети. McAfee Content Security Reporter оптимизирует средства защиты и уменьшает сложность системы обеспечения безопасности ИТ.

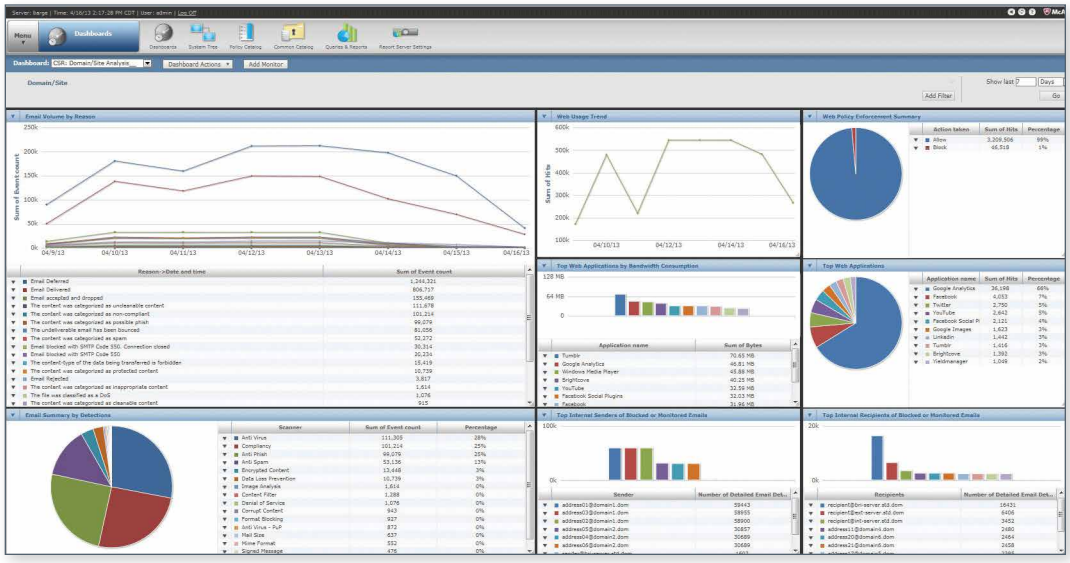

Рис. 1. Контроль электронной почты и веб-трафика с помощью настраиваемых панелей мониторинга

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