Сочетание McAfee Advanced Threat Defense и McAfee Web Gateway

Блокирование скрытых вредоносных программ на периферии сети

Ключевые преимущества

- Автоматическое обнаружение, блокирование и устранение сложных вредоносных программ и атак, скрытых в содержимом веб-страниц.
- В дополнение к веб-защите — настоящий статический анализ кода и анализ кода в «песочнице» с учетом специфики среды без увеличения нагрузки на шлюзы.
- Самонастраиваемые функции блокирования угроз, не требующие вмешательства человека, поэтому работающие без задержки.

Социальные сети, облачные приложения, блоги, вики-ресурсы, RSS-каналы и веб-сайты для обмена разнообразным контентом стали для корпоративных пользователей неотъемлемыми средствами ведения бизнеса, и ИТ-организации всячески стремятся обеспечить безопасность доступа к этим инструментам изнутри и снаружи корпоративной среды. В основе этой работы лежит безопасный веб-шлюз — решение для проверки трафика, сканирующее входящий и исходящий веб-трафик с целью обнаружения и блокирования скрытых угроз.

К сожалению, киберпреступники, стремящиеся использовать уязвимости в растущем объеме корпоративного веб-трафика, работают с не меньшим энтузиазмом, а их атаки становятся все более скрытыми, интеллектуальными, целенаправленным и дорогостоящими. И число атак, успешно обходящих традиционные защитные шлюзы, неизбежно растет.

«Песочница» и защитная «песколовка»

В ответ некоторые организации начинают в дополнение к шлюзам использовать внеполосные аппаратные устройства для динамического анализа кода в «песочнице». «Песочница» запускает подозрительные исполняемые файлы в безопасной виртуальной среде (состоящей из операционной системы, веб-браузера и приложений) и изучает поведение выполняемого кода с целью обнаружения вредоносных намерений. Однако этот кажущийся выигрыш в точности обнаружения часто нивелируется плохой интеграцией и необходимостью принимать меры реагирования вручную.

Например, все, что может сделать большинство сторонних устройств для анализа кода в «песочнице» при обнаружении новой атаки, — это отправить предупреждение специалисту-аналитику. Получив предупреждение, аналитик должен вручную создать новые правила блокировки для шлюза, а затем приступить к задаче поиска и исправления взломанных за это время конечных точек. У существующих «песочниц» есть и другие ограничения:

- дорогостоящее требование иметь по одной выделенной «песочнице» на каждый датчик безопасности, установленный на периметре сети (веб-шлюз, почтовый шлюз, межсетевой экран или IPS);
- наличие одной-единственной, универсальной виртуальной среды выполнения, которая может пропускать атаки, предназначенные для непохожей среды;
- использование только динамического анализа делает «песочницу» уязвимой для интеллектуальных вредоносных программ, которые способны обнаруживать виртуальные среды и откладывать проявление своих намерений.

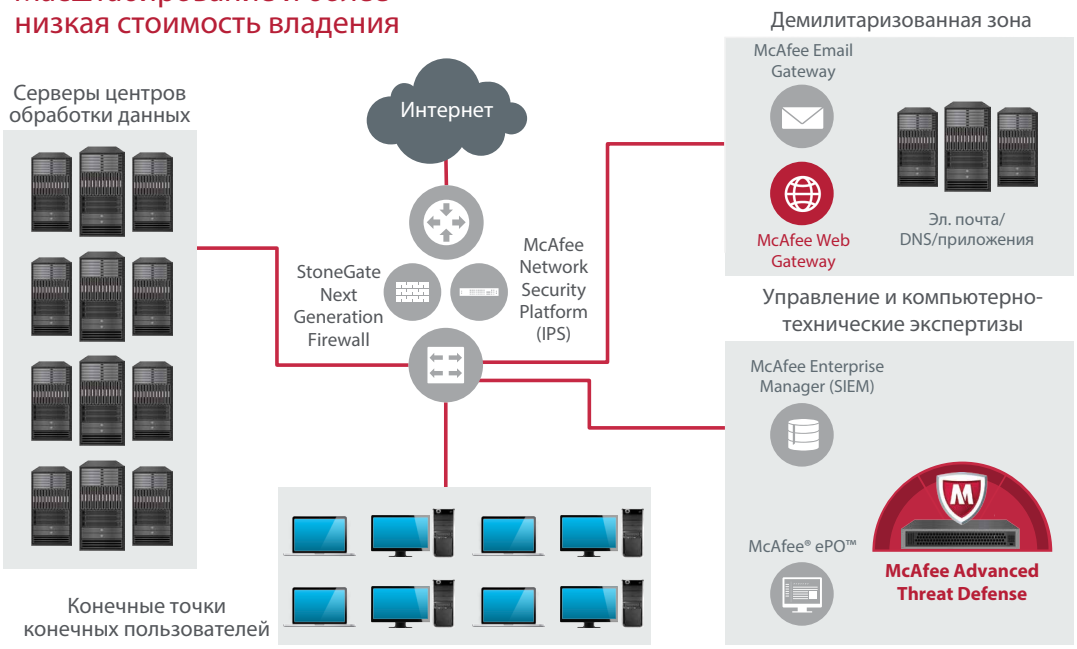
Сочетание веб-шлюза и «песочницы» в рамках концепции Security Connected

Для решения всех этих проблем McAfee® использует сочетание двух тесно интегрированных между собой продуктов: веб-шлюза McAfee Web Gateway, признанного лучшим решением для защиты от веб-угроз, и аппаратного устройства McAfee Advanced Threat Defense, самого эффективного и комплексного из имеющихся в отрасли устройств для обнаружения сложных угроз. Веб-шлюз обеспечивает внутриполосную проверку трафика и блокирование угроз с помощью набора технологий обнаружения вредоносных программ, оптимизированных для работы в режиме реального времени. McAfee Advanced Threat Defense содержит значительный набор средств анализа, обеспечивающих и настоящий статический анализ кода, и анализ кода в «песочнице» с учетом специфики среды. Взаимодействуя друг с другом, эти два устройства обнаруживают, блокируют и устраняют новые, неизвестные и скрытые угрозы повышенной сложности.

- *Обнаружение.* Использование новаторских технологий анализа позволяет быстро и точно обнаруживать изощренные угрозы в большом количестве разных протоколов.
- *Блокирование.* Тесная интеграция с защитными продуктами McAfee позволяет мгновенно блокировать попытки проникновения в сеть и изолировать зараженные конечные точки.
- *Устранение.* Данное решение автоматически сканирует всю среду на наличие проникнувших в нее угроз и инициирует процесс устранения уязвимостей конечных точек.

Централизованное развертывание

Масштабирование и более низкая стоимость владения



Поскольку данное решение соответствует принципам интеграции корпоративных средств защиты, изложенным в концепции McAfee Security Connected, оно обеспечивает ряд преимуществ, не имеющих себе равных в отрасли с точки зрения эффективности эксплуатации и защиты:

- *Самонастраиваемые функции блокирования угроз.* McAfee Web Gateway автоматически блокирует атаки, которые обнаруживает McAfee Advanced Threat Defense, что позволяет избавиться от задержек, вызываемых вмешательством человека.
- *Единая централизованная служба анализа кода в «песочнице».* McAfee Advanced Threat Defense может одновременно поддерживать и другие системы сетевой безопасности (шлюзы электронной почты, межсетевые экраны, системы предотвращения вторжений и др.). Это снижает затраты, упрощает архитектуру безопасности и сокращает время реагирования, проходящее с момента обнаружения новой атаки до ее блокирования в масштабе всей сети.
- *Сверхэффективный процесс проверки.* Аппаратные веб-шлюзы выполняют первоначальную фильтрацию и направляют в «песочницу» только то содержимое трафика, которое не может быть проанализировано шлюзом.
- *«Песочница», учитывающая специфику среды.* McAfee Advanced Threat Defense каждый раз подбирает такую виртуальную среду выполнения, которая соответствует системе целевого узла. Это повышает точность обнаружения и сокращает как время анализа, так и количество ложных положительных результатов.
- *Интеграция отчетов и рабочих процессов.* Отчеты, которые генерирует McAfee Advanced Threat Defense, автоматически интегрируются в рабочие процессы McAfee Web Gateway, благодаря чему пользователи получают обратную связь и результаты сканирования.

Описание McAfee Web Gateway

McAfee Web Gateway — это ведущее отраслевое решение для борьбы с вредоносными программами, используемое организациями в качестве первой линии обороны против постоянно эволюционирующих веб-угроз. Оно дает организациям возможность с помощью политик гибко регулировать доступ пользователей к веб-приложениям и ресурсам, значительно снижая при этом уровень риска, которому подвергаются внутренние системы и информация.

Сначала McAfee Web Gateway принудительно применяет ко всем инициированным пользователем веб-запросам внутреннюю политику доступа, а затем с помощью ряда локальных и глобальных методов проверки в режиме реального времени выявляет природу и намерения всего содержимого веб-трафика. В качестве средств анализа для обнаружения угроз используются антивирус на базе сигнатур и служба McAfee Global Threat Intelligence (McAfee GTI), предоставляющая результаты анализа репутации (файла и источника), классификации и геолокации. Наконец, в McAfee Web Gateway используется запатентованная методика упреждающего обнаружения вредоносных программ «нулевого дня», позволяющая путем эмуляции и эвристического анализа прогнозировать поведение

и выявлять намерения (исполняемого) файла. Декодированию и проверке на скрытые атаки подвергается даже информация, зашифрованная с помощью SSL. Это позволяет получить крайне высокий процент обнаружения и дает возможность мгновенно блокировать атаки на шлюзе в упреждающем режиме. Как показывают результаты независимых тестов, McAfee Web Gateway выявляет и блокирует 95–99 % вредоносных программ «нулевого дня».

Кроме того, McAfee Web Gateway обеспечивает защиту исходящего трафика путем сканирования создаваемого пользователями контента по всем основным веб-протоколам (HTTP, HTTPS и FTP). Это позволяет предотвращать утечки конфиденциальной информации, происходящие в результате непреднамеренной ошибки пользователя или скрытых действий узла, зараженного ботом. Интегрированная поддержка политик предотвращения утечки данных (DLP) позволяет блокировать попытки вывода регулируемых и конфиденциальных данных за пределы сети, а встроенный механизм шифрования файлов обеспечивает защиту информации, загружаемой на внешние файлообменные сайты и сайты для совместной работы, такие как Box, Dropbox и др.

Самой ценной особенностью McAfee Web Gateway является возможность его интеграции с другими решениями. Это дает ему доступ к аналитической информации и функциям других продуктов McAfee. В случае данного решения особое значение имеет прямая интеграция со следующими технологиями:

- службой McAfee Global Threat Intelligence, которая собирает, анализирует и распространяет информацию о репутации URL-адресов и другие данные, получаемые с более чем 100 миллионов конечных точек в 120 странах. Эта служба дает пользователям возможность с точностью до минуты получать данные о веб-сайтах, зараженных вредоносным ПО;
- программным обеспечением Real Time for McAfee ePolicy Orchestrator® (McAfee ePO™), позволяющим в режиме реального времени собирать информацию о конечных точках и управлять ими с целью изолирования успешных атак и устранения уязвимостей;
- McAfee Enterprise Security Manager, революционным решением для управления информацией о безопасности и событиях безопасности (security information and event management — SIEM), позволяющим в режиме реального времени получать информацию о внутренней ИТ-среде, сочетаемую и сопоставляемую с данными о глобальном контексте, получаемыми из внешнего мира. Тщательно настроенная база данных McAfee Enterprise Security Manager собирает миллиарды журнальных событий и сопоставляет их с другими важными потоками данных, что позволяет мгновенно получать доступ к данным о событиях безопасности за много лет. Рассчитывая базовые уровни для всех входящих потоков данных, она выявляет аномалии и потенциальные угрозы, не давая им развиться, и упрощает процесс управления нормативно-правовым соответствием благодаря наличию сотен готовых панелей мониторинга и шаблонов отчетов;
- McAfee Advanced Threat Defense — компонентом данного решения, отвечающим за обнаружение сложных вредоносных программ.

Описание «песочницы»: McAfee Advanced Threat Defense

McAfee Advanced Threat Defense представляет собой многоуровневое решение для обнаружения вредоносных программ, в котором используется расширяемый набор контрольных модулей и аналитических функций, расположенных в порядке возрастания интенсивности вычислений. Такой уникальный подход к получению полной и при этом эффективной оценки угроз позволяет обеспечить очень высокий уровень точности обнаружения и надежности работы при крайне высокой пропускной способности. В McAfee Advanced Threat Defense встроены следующие средства анализа:

- *Средства полного статического анализа кода*, которые выполняют обратную разработку кода файла, позволяющую провести оценку всех атрибутов и наборов инструкций и полностью проанализировать исходный код без его выполнения. Универсальные функции распаковки файлов открывают все виды упакованных и сжатых файлов, что позволяет проводить полный анализ и классификацию вредоносных программ. В результате организации получают возможность лучше разобраться в угрожающих им вредоносных программах и понять, в чем их опасность. Полный статический анализ кода дает критически важную информацию о поведении кода, зависящем от вводимых данных, и о скрытых путях (отложенного) выполнения кода, которые во время динамического анализа часто не выполняются и не попадают в поле зрения менее совершенных «песочниц».
- *Средства динамического анализа кода в «песочнице»*, которые выполняют код файла в виртуальной среде выполнения и наблюдают за его поведением. В отличие от всех других существующих «песочниц» McAfee Advanced Threat Defense настраивает виртуальные среды выполнения в соответствии с особенностями целевого узла, посылая для этого запросы к программному обеспечению McAfee ePO. Он может хранить и использовать пользовательские «золотые» образы и поддерживает большое количество разных типов виртуальных машин. Анализ поведения файла в условиях, точно соответствующих условиям того узла, для которого файл предназначен, позволяет быстро и эффективно получать точные результаты и выявлять такие сценарии вредоносного поведения, которые не могут проявиться при запуске в универсальной среде. А поскольку многие сложные атаки способны избегать обнаружения в «песочнице», в McAfee Advanced Threat Defense используются инновационные методы, гарантирующие выполнение кода в ходе его динамического анализа.

McAfee Security Connected

Платформа Security Connected компании McAfee представляет собой единую структуру, в рамках которой сотни продуктов, услуг и партнеров могут обмениваться друг с другом важными сведениями, в режиме реального времени делиться друг с другом данными о контексте и совместно обеспечивать безопасность информации и сетей. Используя предлагаемые данной платформой инновационные концепции, оптимизированные процессы и практические рекомендации, любая организация может понизить уровень риска, сократить время реагирования на инциденты и снизить расходы на администрирование и обслуживающий персонал.

Скоординированное использование этих методов позволяет эффективно выявлять большое количество разных видов известных и неизвестных вредоносных программ. Сочетание полного статического анализа и динамического анализа дает возможность обнаруживать замаскированное и сложное вредоносное ПО, не выявляемое с помощью легковесных аналитических модулей. Возможность задавать, на какое время будет запаздывать доставка анализируемого контента, позволяет специалистам по безопасности регулировать время ожидания и размер принимаемого риска.

Предел пропускной способности аппаратных устройств McAfee Advanced Threat Defense — 250 000 объектов в день. Это дает возможность поддерживать большое количество датчиков безопасности сети с помощью одной системы защиты от сложного вредоносного ПО. Устройствами McAfee Advanced Threat Defense, как и всеми решениями сетевой безопасности McAfee, можно управлять централизованно через веб-интерфейс, предоставляемый устройством McAfee Network Security Manager.

Эффективное решение замкнутого цикла для предотвращения сложных угроз

Сочетание McAfee Web Gateway и McAfee Advanced Threat Defense обеспечивает исключительно эффективную защиту от сложных вредоносных программ, распространяемых посредством веб-трафика. Это автоматизированное решение замкнутого цикла обнаруживает изощренные атаки, останавливает их распространение и устраняет уязвимости затронутых ими систем, не требуя ручного вмешательства со стороны ИТ-персонала, и без того перегруженного работой.

За дополнительной информации о том, как с помощью решений McAfee защитить сеть организации от скрытых сложных угроз, обращайтесь к представителю McAfee или на страницу www.mcafee.com/ru/products/advanced-threat-defense.aspx.

McAfee
An Intel Company

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной», Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.McAfee.ru

61133brf_atd-web-gateway_0614_fnl_ETMG