Сочетание McAfee Advanced Threat Defense и системы предотвращения сетевых вторжений

Обеспечение более широкой защиты от скрытых вредоносных программ

Ключевые преимущества

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

Система предотвращения сетевых вторжений (IPS) составляет основу любой корпоративной архитектуры безопасности. Развернутые внутриполосно в сочетании со средствами защиты на шлюзах и узлах, системы IPS осуществляют мониторинг сетевого трафика и поведения конечных точек, используя целый ряд методов для обнаружения атак и активации мер реагирования.

Однако в настоящее время растет число неизвестных угроз «нулевого дня», которым удается успешно обходить традиционные средства защиты. Будучи скрытыми, хорошо замаскированными, автоматически адаптирующимися и зачастую тщательно спланированными, эти изощренные атаки представляют собой небольшой, но непропорционально опасный и дорогостоящий фрагмент постоянно меняющейся картины угроз.

В ответ на это некоторые организации начинают в дополнение к уже имеющейся у них инфраструктуре IPS использовать внеполосные аппаратные устройства для динамического анализа кода в «песочнице». «Песочница» запускает подозрительные исполняемые файлы в безопасной виртуальной среде и изучает поведение выполняемого кода с целью обнаружения вредоносных намерений. Часто, однако, этот кажущийся выигрыш в точности обнаружения быстро 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 IPS и межсетевого экрана, а затем приступить к задаче выявления и исправления всех конечных точек, взломанных за время проведения внеполосного анализа кода в «песочнице». У существующих решений есть и другие распространенные ограничения:

- дорогостоящее требование иметь по одной «песочнице» на каждый датчик IPS;
- использование универсальной виртуальной среды выполнения, которая может оказаться не в состоянии выявить сценарии поведения, предназначенные исключительно для атакуемой среды;
- использование только динамического анализа, что делает «песочницу» уязвимой по отношению к разным стратегиям, используемым вредоносными программами для обнаружения защищенных сред и временного отказа от проявления своих намерений.

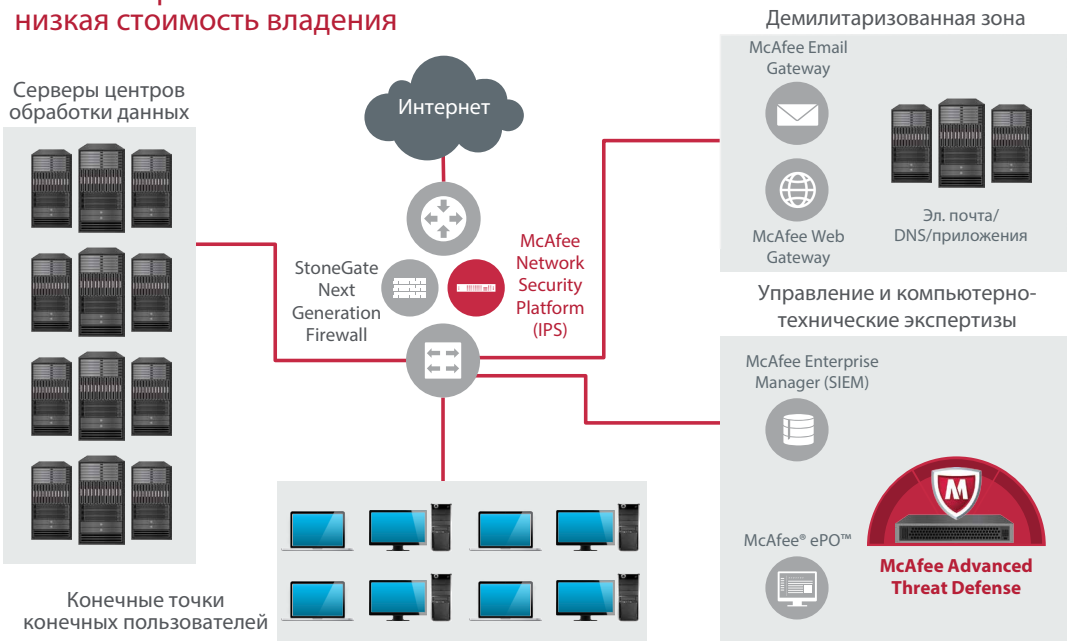
Сочетание IPS и «песочницы» в рамках концепции Security Connected

Для решения всех этих проблем McAfee предлагает использовать сочетание двух тесно интегрированных между собой продуктов: платформы McAfee Network Security Plattform, представляющей собой современный быстродействующий датчик IPS, и аппаратного устройства McAfee Advanced Threat Defense, самого эффективного и комплексного из имеющихся в отрасли устройств для обнаружения сложных вредоносных программ. McAfee Network Security Platform 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 более широкий и ресурсоемкий 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 и блокируют новые, неизвестные и скрытые угрозы повышенной сложности. Чтобы получить комплексное решение, добавьте к ним Real Time for McAfee ePO, позволяющий быстро обнаруживать и восстанавливать любые системы, пострадавшие от сложного вредоносного ПО.

- *Обнаружение.* Использование новаторских технологий анализа позволяет быстро и точно обнаруживать современные изощренные угрозы в большом количестве разных протоколов.
- *Блокирование.* Тесная интеграция с сетевыми шлюзами McAfee позволяет мгновенно блокировать дальнейшие попытки проникновения в сеть и изолировать зараженные конечные точки.
- *Устранение.* Данное решение McAfee автоматически отслеживает случаи проникновения угроз в масштабах всей среды и инициирует процесс устранения уязвимостей конечных точек.

Централизованное развертывание

Масштабирование и более низкая стоимость владения



Поскольку сочетание McAfee Advanced Threat Defense с системой предотвращения сетевых вторжений соответствует принципам интеграции корпоративных средств защиты, изложенным в концепции Security Connected, оно обеспечивает ряд преимуществ, не имеющих себе равных в отрасли с точки зрения эффективности эксплуатации и защиты:

- *Самонастраиваемые функции блокирования угроз.* McAfee Network Security Platform автоматически блокирует атаки, которые обнаруживает McAfee Advanced Threat Defense, что позволяет избавиться от задержек, вызываемых вмешательством человека.
- *Интеграция отчетов и рабочих процессов.* Отчеты, которые генерирует McAfee Advanced Threat Defense, автоматически интегрируются в рабочие процессы McAfee Network Security Platform, что позволяет избежать необходимости при проведении расследований постоянно переключаться между разными панелями.
- *Сбор информации о конечных точках.* McAfee Advanced Threat Defense может получать доступ к любой информации о конечных точках, хранящейся в McAfee Network Security Platform, и использовать ее для повышения скорости и точности обнаружения угроз.

Система IPS: McAfee Network Security Platform

McAfee Network Security Platform — это семейство комплексных систем предотвращения вторжений (IPS) в виде аппаратных устройств, обнаруживающих и блокирующих попавшие в сеть изощренные угрозы: сложные вредоносные программы, угрозы «нулевого дня», атаки типа «отказ в обслуживании», бот-сети и т. п. Используя сверхэффективную архитектуру однопроходной углубленной проверки трафика и специальное аппаратное обеспечение операторского класса, McAfee Network Security Platform с помощью одного-единственного устройства обеспечивает высокую скорость передачи данных (до 40 Гбит/с) и поддерживает исключительно высокий уровень пропускной способности и точности независимо от настроек безопасности. В платформу встроены функции проведения следующих видов анализа: пользовательские сигнатуры, полный анализ протоколов, анализ репутации угроз, глубокий анализ файлов с использованием эмуляции и средств обнаружения JavaScript, а также сопоставление поведения угроз с данными об использовании приложений (платформа способна отслеживать более 1 500 приложений и протоколов 7-го уровня).

Вместе лучше

- Максимизируйте отдачу от уже сделанных инвестиций в обеспечение безопасности.
- Избавьтесь от необходимости полностью менять архитектуру сети.
- Расширьте и автоматизируйте защиту.
- Сведите к минимуму работу по устранению уязвимостей и расследованию инцидентов, используя надежные функции блокирования угроз в потоке.
- Оптимизируйте рабочие процессы с помощью интерфейса McAfee Network Security Platform.

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.

Самой ценной особенностью платформы McAfee Network Security Platform является, пожалуй, ее способность интегрироваться с другими решениями McAfee с целью использования имеющихся у них функций и собираемой ими информации. В данном случае особое значение имеет возможность прямой интеграции со следующими технологиями:

- 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.

«Песочница»: 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:

- Обнаружение вирусов, червей, шпионских программ, ботов, троянский коней, переполнения буфера и смешанных атак с помощью обширной базы знаний KnowledgeBase, созданной и регулярно пополняемой сотрудниками McAfee Labs и на данный момент содержащей почти 150 миллионов сигнатур.
- Обнаружение только что возникших угроз с помощью данных о репутации, получаемых из сети McAfee Global Threat Intelligence.
- Статический анализ и эмуляция в режиме реального времени, позволяющие быстро находить вредоносные программы и угрозы «нулевого дня», не выявленные с помощью сигнатур и данных о репутации.
- 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 имеющихся на сегодняшний день «песочниц» McAfee Advanced Threat Defense настраивает виртуальные среды выполнения в соответствии с особенностями целевого узла, посылая для этого запросы к программному обеспечению McAfee ePO. 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. Поскольку многие передовые атаки способны избегать обнаружения в «песочнице», в McAfee Advanced Threat Defense используются инновационные методы, гарантирующие выполнение кода в ходе его динамического анализа.

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.

Устройства McAfee Advanced Threat Defense можно легко настроить на выполнение только тех видов анализа, которые не были выполнены предшествующими датчиками IPS, исключив тем самым риск снижения производительности из-за проведения избыточных проверок. Предел пропускной способности аппаратных устройств McAfee Advanced Threat Defense — 250 000 объектов в день. Это дает возможность поддерживать большое количество датчиков McAfee Network Security Platform с помощью одной системы защиты от сложного вредоносного ПО. Для централизованного управления устройствами McAfee Advanced Threat Defense и платформой McAfee Network Security Platform используется веб-интерфейс, предоставляемый устройством McAfee Network Security Manager.

Эффективное решение замкнутого цикла для предотвращения сложных угроз

Сочетание McAfee Network Security Platform и McAfee Advanced Threat Defense обеспечивает крайне эффективную защиту от сетевых вторжений, а также позволяет крайне эффективно обнаруживать сложные вредоносные программы и принимать меры реагирования. Это автоматизированное решение замкнутого цикла обнаруживает изощренные атаки, останавливает их распространение и устраняет уязвимости затронутых ими систем, не требуя ручного вмешательства со стороны операторов сети или аналитиков безопасности, и без того перегруженных 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.

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

61051brf_atd-network-ips_0514_fnl_ETMG