Краткий обзор решения

Слаженная безопасность

Адаптивный механизм сбора информации об угрозах дает возможность незамедлительно реагировать на новые угрозы.

Стремясь создать эффективную систему защиты от новых современных угроз, организации сталкиваются с большим количеством проблем в области безопасности и целым рядом задач оперативного характера. В атаках «нулевого дня» и в сложных целенаправленных атаках используются ранее неизвестные методы. Аналогичную проблему представляют собой полиморфные вредоносные программы. Если использовать только традиционные меры противодействия на основе сигнатур, то обнаружение сложного вредоносного содержимого будет затруднено.

Для эффективной борьбы с новыми угрозами организациям необходима такая система безопасности, которая сочетает в себе средства анализа поведения, оценки репутации и использования сигнатур как в сети, так и на конечных точках. И хотя каждая из этих технологий сама по себе хорошо справляется с задачей выявления угроз, важно, чтобы они работали сообща, обмениваясь информацией и совместно подстраиваясь под меняющиеся угрозы. Передачу информации между решениями для защиты сети и конечных точек можно осуществлять вручную, но это трудоемко и не обеспечивает той скорости, которая необходима для борьбы с современными угрозами.

Взаимодействуя друг с другом, McAfee® Threat Intelligence Exchange и McAfee Advanced Threat Defense совместными усилиями обеспечивают автоматизированную адаптивную защиту от новых угроз. Независимо от того, где имел место первый контакт с неизвестным вредоносным файлом, после подтверждения его вредоносного статуса информация о нем немедленно распространяется по всей сети компании. Когда McAfee Advanced Threat Defense проводит анализ файла, McAfee Threat Intelligence Exchange предоставляет результаты этого анализа всем имеющимся в организации средствам защиты. Для рассылки этой информации используется уровень обмена данными. Благодаря этому конечные точки, подключенные к McAfee Threat Intelligence Exchange, будут защищены от этого файла в случае его появления в будущем. А шлюзы, подключенные к McAfee Threat Intelligence Exchange, не допустят этот файл внутрь организации. Кроме того, когда конечные точки, подключенные к McAfee Threat Intelligence Exchange, сталкиваются с файлами с неизвестной репутацией, они направляют эти файлы в McAfee Advanced Threat Defense, чтобы определить, является ли данный объект вредоносным. Это позволяет избежать дальнейшей неопределенности, связанной с такими файлами.

Устранение бреши в защите

Выявление трафика, содержащего вредоносные программы
Взаимодействуя друг с другом, McAfee Threat Intelligence Exchange и McAfee Advanced Threat Defense совместно анализируют подозрительные объекты независимо от того, где файл был обнаружен впервые. При попытке запуска новые файлы подвергаются комплексному анализу, проводимому взаимосвязанными компонентами этого объединенного решения. Для анализа используются правила конечных точек, локальная и глобальная информация о репутации,

Ключевые преимущества

- Резкое сокращение времени, необходимого для локализации угроз, благодаря механизму автоматизированного адаптивного реагирования на угрозы
- Возможность лучше и быстрее отслеживать и контролировать ситуацию благодаря взаимодействию конечных точек в сети
- Интеллектуальное реагирование на обнаруживаемые файлы благодаря наличию однозначной информации о репутации и выполнении файлов
- Повышение уровня безопасности и оптимизация совокупной стоимости владения средствами защиты благодаря упрощению процессов их интеграции и внедрения

intel Security

а также средства углубленного статического и динамического анализа. Такой комплексный подход к анализу угроз позволяет точнее выявлять скрытые вредоносные программы, которые в противном случае могли бы остаться незамеченными.

Более эффективное обнаружение угроз путем анализа поведения
McAfee Advanced Threat Defense дает возможность классифицировать репутацию файлов с помощью инновационных функций деконструирования вредоносных программ. К ним относится, например, функция распаковки, позволяющая обойти методы обхода защиты и добраться до исходного исполняемого кода с целью выявления его потенциальных действий. Сочетание статического анализа кода и динамического анализа позволяет проводить полную оценку файла и представляет собой самую надежную из имеющихся на рынке технологий обнаружения сложных угроз.

Возможность отслеживать и контролировать происходящее на конечных точках и в сети
Кроме того, McAfee Advanced Threat Defense получает образцы вредоносных программ, собираемые в точках входа в сеть другими продуктами, установленными в сети компании. В свою очередь, эти компоненты сети могут посредством McAfee Threat Intelligence Exchange обмениваться между собой информацией, полученной в результате анализа этих образцов. Такой обмен информацией об угрозах и репутации между конечными точками в пределах сети является хорошей демонстрацией принципа функционирования платформы Security Connected, разработанной компанией McAfee. А наличие базы знаний с информацией о месте и времени выполнения объектов на конечных точках дает McAfee Threat Intelligence Exchange возможность поставлять однозначную информацию о недавно появившихся угрозах.

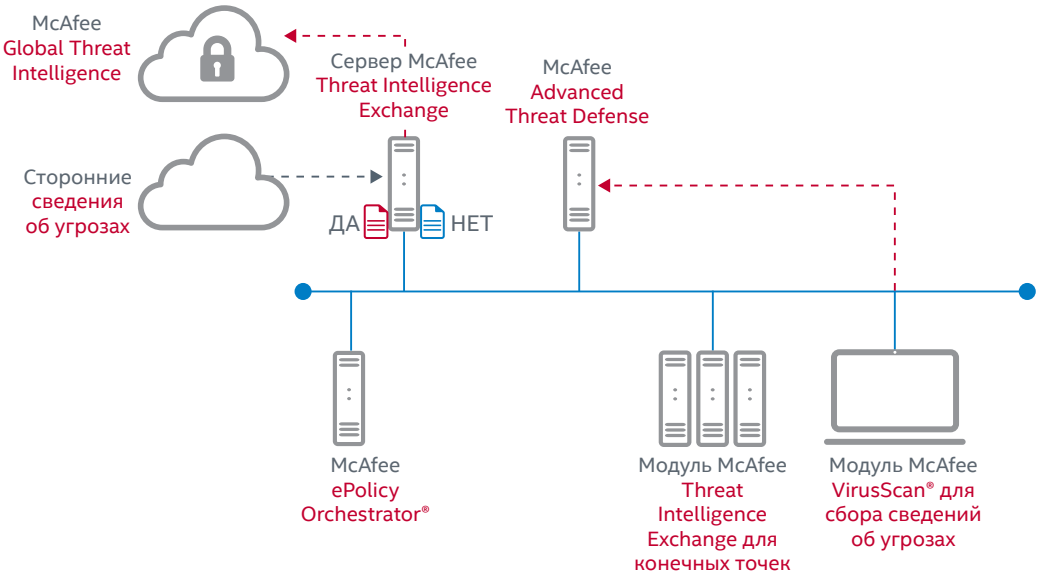

Рис. 1. Синтез информации об угрозах и репутации на основе данных, получаемых из облака, сети и конечных точек

Адаптивное реагирование

После анализа и классификации файла в McAfee Advanced Threat Defense полученные результаты направляются в McAfee Threat Intelligence Exchange. Информация о репутации нового файла, независимо от того, хорошая она или плохая, сразу рассылается всем имеющимся в среде средствам защиты, подключенным к McAfee Threat Intelligence Exchange. Теперь все экземпляры данного файла будут сразу распознаваться, а все компоненты, подключенные к McAfee Threat Intelligence Exchange, будут принимать меры в соответствии с политикой: допускать, блокировать или удалять этот файл. Такой адаптивный процесс реагирования позволяет моментально обеспечивать защиту всей среды, включая сеть, шлюзы

В основе Security Connected — уровень обмена данными McAfee
McAfee Threat Intelligence Exchange — первое решение, использующее уровень обмена данными McAfee, представляющий собой быструю, легковесную и двунаправленную коммуникационную систему и позволяющий организовать сбор информации об угрозах и построить адаптивную систему безопасности благодаря простоте интеграции продуктов и обмену контекстной информацией. Продукты, соединенные между собой посредством уровня обмена данными McAfee, могут получать и распространять информацию через этот канал, просто подписавшись на него. Не нужно ни сложных программных интерфейсов (API), ни утомительного конфигурирования. Он знаменует собой новую эру в разработке систем безопасности, когда все компоненты объединяются и взаимодействуют как единая, слаженная система.

и конечные точки. Таким образом, скорость реагирования повышается, а время, необходимое для локализации и устранения угрозы, резко сокращается, и для этого не требуется менять архитектуру сети.

Простота развертывания и управления

Интеграция McAfee Threat Intelligence Exchange и McAfee Advanced Threat Defense осуществляется посредством уровня обмена данными. Благодаря своей открытости уровень обмена данными дает компонентам системы безопасности возможность динамически подключаться к McAfee Threat Intelligence Exchange. Это избавляет организации от необходимости использовать многофункциональные API и создавать сложные конфигурации продуктов, что, в свою очередь, приводит к уменьшению количества ошибок и сокращению объема операций, выполняемых вручную.

ВЗАИМОСВЯЗЬ
Легко реализуемая интеграция сетевых устройств и конечных точек, позволяющая им слаженно взаимодействовать и обмениваться информацией о безопасности

ЗАЩИТА
Использование всех взаимосвязанных средств защиты для анализа подозрительных объектов независимо от того, где была точка первого контакта

РЕАГИРОВАНИЕ
Беспрецедентно подробное изучение обнаруженных объектов и анализ прошлых событий с помощью централизованной базы данных об угрозах, позволяющей полностью контролировать происходящее в среде

АДАПТАЦИЯ
Автоматизированное, немедленное и согласованное реагирование на возникающие угрозы на всех конечных точках и сетевых устройствах

Рис. 2. Интеграция компонентов Security Connected посредством уровня обмена данными

Дополнительная информация

McAfee Threat Intelligence Exchange и McAfee Advanced Threat Defense необходимы для интеграции между собой разнородных компонентов системы безопасности, защиты среды, реагирования на обнаруживаемые объекты и автоматической адаптации средств защиты к возникающим угрозам. Предлагая экосистему защиты, сочетающую в себе передовые средства анализа угроз, сетевые продукты и решения для конечных точек, McAfee дает возможность получать информацию о происходящем и собирать контекстные данные об угрозах в масштабах всей организации. Помимо сказанного, решение позволяет сократить время реагирования на инциденты и упростить процесс устранения уязвимостей.

- **http://www.mcafee.com/ru/products/threat-intelligence-exchange.aspx**
- **http://www.mcafee.com/ru/products/advanced-threat-defense.aspx**
- **http://www.mcafee.com/ru/enterprise/security-connected/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