McAfee Network Security Platform: объединение безопасности сети и безопасности системы

Платформа сетевой безопасности уровня предприятия

McAfee Network Security Platform предоставляет беспрецедентную безопасность, управляемую знаниями. Помимо системы управления рисками в системе безопасности (SRM) McAfee, Network Security Platform работает совместно с McAfee Foundstone®, McAfee ePolicy Orchestrator® (ePO™) и McAfee Network Access Control (NAC), формируя интеллектуальную систему защиты в реальном времени, во много раз более точную и эффективную, чем традиционные точечные продукты.

Основные преимущества

McAfee SRM

- Интеграция с McAfee Foundstone и McAfee ePO принесла не только обнаружение и предотвращение вторжений: появились такие возможности, как предоставление критических параметров узла, оценка по требованию релевантности угрозы и риска, а также карантин узла.

Инфраструктура безопасности McAfee, предусматривающая совместную работу

- Структура управления рисками нарушения безопасности, разработанная McAfee, предусматривает совместную работу, объединяя безопасность сети и системы. Это позволит вам воспользоваться преимуществами существующей экосистемы безопасности — выполнять больший объем работы с меньшими усилиями.

Компания McAfee открывает пространство ценностей и преимуществ интеграции для получения эффекта от инвестиций в безопасность. Интеграция сетевой (Network Security Platform) и системной (ePO) инфраструктур безопасности приводит к созданию единой системы предотвращения вторжений, учитывающей информацию о системе, обеспечивающей эффективное взаимодействие в сфере безопасности для предоставления полной картины системных и сетевых угроз. Прорывное решение ePolicy Orchestrator® обеспечивает в реальном времени полную картину сведений об узлах, требующих принятия мер, а также наиболее важных событиях Host IPS и программ защиты от вирусов/шпионских программ.

Интеграция с McAfee Foundstone обеспечивает в реальном времени предоставление по запросу информации о значимости угроз. Точная информация относительно значимости угроз и хорошая осведомленность дают вам возможность принимать быстрые и эффективные меры по их устранению.

Интеграция с McAfee NAC распространяет сферу доступности и глубину применения политик, предоставляя динамический контроль доступа нулевого дня. Благодаря использованию в сочетании со встроенной возможностью карантина узла в Network Security Platform (NSP), динамический NAC обеспечивает постоянный контроль до и после входа для управляемых, неуправляемых и не подлежащих управлению узлов.

Управляемая знаниями безопасность сети

Интеллектуальная интеграция защиты сети и системы обеспечивает безопасность в реальном времени, которая не только автоматизирована, но и позволяет выполнять дальнейшие действия. С помощью одного щелчка мыши вы получаете интеллектуальную систему предотвращения вторжений, предоставляющую по запросу критическую информацию об узлах, наиболее важных вторжениях на узел и атаках шпионских программ, а также точное определение релевантности угрозы и риска. Решение реального времени для обеспечения защиты позволяет принимать решения относительно безопасности в реальном времени, обеспечивая более короткое время на обеспечение защиты и уверенности.

Интеграция с ePO
Меньшее время на защиту/на решение проблемы с видимостью в реальном времени сведений об узлах системы, самых серьезных атаках Host IPS и событий программы защиты от вирусов/шпионских программ

Интеграция с Foundstone
IPS реального времени с информацией о рисках, с функцией проверки значимости угроз по запросу и функцией Foundstone «Сканировать сейчас»

Интеграция с McAfee NAC
Карантин узла на основе поведения и динамический NAC для контроля в реальном времени управляемых и неуправляемых узлов после входа

Анализ угроз в режиме реального времени. Действия по обеспечению безопасности в реальном времени

Возможности предоставления в реальном времени данных по релевантности, видимости и контролю дают возможность принимать эффективные решения по обеспечению безопасности в реальном времени для сокращения времени на защиту и времени на обеспечение соответствия.

Знание о безопасности, дающее возможность действовать

Интеграция сетевой и системной безопасности усиливает все точки видимости — включая McAfee Foundstone, ePO и NAC, — чтобы обеспечить управляемую знаниями безопасность, которая во много раз действеннее и точнее специализированных продуктов IPS.

Меньше времени на обретение уверенности
Компания McAfee интегрировала несколько продуктов и технологий для того, чтобы можно было различить шум и значимую информацию в реальном времени. Такую уверенность в безопасности может обеспечить только платформа McAfee Network Security Platform.

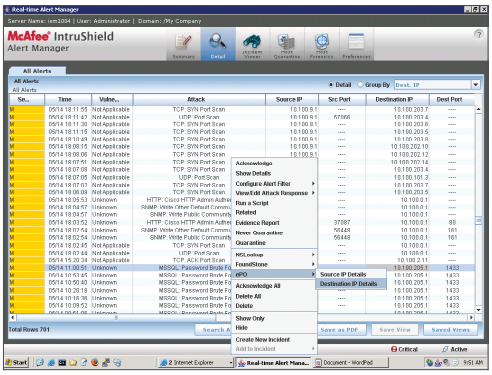
Интеграция с ePO: IPS в реальном времени с использованием информации о системе

Обычным щелчком правой кнопкой мыши в диспетчере Network Security Platform можно получить сведения об узле источника или узле назначения. Пользователь получает полную видимость такой информации как имя узла, имя пользователя, текущая защита этого узла и 10 самых важных событий вторжения, произошедших на нем.

Это дает администратору сети непосредственную, действенную информацию, которая никогда ранее не предоставлялась сетевому администратору до интеграции компанией McAfee решений Network Security Platform и ePO.

Интеграция структуры управления рисками нарушения безопасности и McAfee ePO

Система предотвращения вторжений реального времени, учитывающая информацию о системе и обеспечивающая видимость в масштабах предприятия



Система предотвращения вторжений со сведениями о системе вместе с данными узлов из ePO

- Обычный щелчок правой кнопкой предоставляет информацию в реальном времени об IP-адресах компьютера источника или назначения
- Предоставляет имя узла, имя пользователя, ОС, уровень пакета исправлений, MAC-адрес, последнюю дату проверки и прочие политики защиты, 10 самых серьезных событий вторжения на узел

Преимущества системы предотвращения вторжений со сведениями о системе

- Меньше времени на обретение уверенности
- Видимость, эффективность, релевантность
- Эффективное использование инвестиций в ePO

Как это работает?

Интегрирование Network Security Platform и ePO дает вам возможность послать запрос базе данных ePO о подробных характеристиках узлов вашей сети прямо из Alert Manager. Информация, получаемая из базы данных ePO включает тип узла, имя узла, сведения об операционной системе и о продуктах для обеспечения безопасности системы, установленных на данном узле. Если в рамках установки ePO было установлено решение McAfee Host Intrusion Prevention, это дает вам возможность просматривать последние 10 событий HIPS для конкретного узла. Такая информация расширяет видимость и релевантность информации для администраторов безопасности, выполняющих экспертизу событий системы безопасности, замеченных в сети.

Для лучшего понимания совместной работы Network Security Platform и ePO необходимо рассматривать следующий сценарий. В Alert Manager вы замечаете, что один из узлов вашей сети сканирует порты других узлов. Вам необходимо получить более подробную информацию об этих атаках. Вы щелкаете правой кнопкой мыши на предупреждении и видите развернутую информацию об IP источника. NSP опрашивает базу данных ePO и отображает информацию об узле в Alert Manager. Исходя из этой информации вы понимаете, что VirusScan (антивирусное приложение McAfee) устарело. Глядя на имя узла, вы приходите к выводу, что это сервер, некоторое время назад исключенный из сети. Таким образом, VirusScan в течение этого времени не обновлялся.

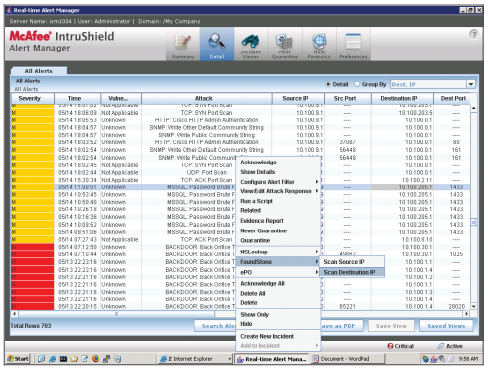
Интеграция с Foundstone: IPS в реальном времени с информацией о рисках

Оценка уязвимости — это автоматизированный процесс упреждающей идентификации уязвимостей компьютерных систем сети с целью определения угроз в сети. Network Security Platform обеспечивает интеграцию Foundstone Enterprise. Вы можете запросить удаленную проверку и использовать отчеты об оценке уязвимости, полученные от сканеров, для определения релевантности атак на узлы.

Network Security Platform была интегрирована со сканером уязвимости Foundstone Enterprise. В этой расширенной интегрированной системе присутствуют два основных компонента. Во-первых, пользователи могут планировать импорт результатов сканирования Foundstone в Network Security Platform с целью автоматического обновления релевантных данных об IPS-событиях. Во-вторых, пользователи имеют возможность запустить сканирование по требованию Foundstone одного или группы IP-адресов прямо с консоли Alert Manager NSP. Это дает администраторам безопасности простой способ доступа к информации об уязвимостях узла практически в реальном времени, а также фокусирует их внимание на критических событиях.

Интеграция структуры управления рисками нарушения безопасности и McAfee Foundstone

IPS в реальном времени с информацией о рисках



Функции IPS в реальном времени с информацией о рисках

- Автоматический импорт отчетов о проверках Foundstone.
- Функция Foundstone «Сканировать сейчас» предоставляет по запросу результаты проверки значимости, отсортированные по узлам.

Преимущества использования IPS с информацией о рисках в реальном времени

- Улучшенная концентрация внимания на критических событиях
- Автоматизация, точное определение значимости
- Обновление в реальном времени информации об уязвимости для определенных узлов

Как это работает?

Сканирование по требованию. Из Alert Manager NSP вы можете послать запрос Foundstone на выполнение сканирования, ядро FoundScan сканирует узел и предоставляет данные по оценке уязвимости на Network Security Platform. Эта информация обрабатывается и хранится в базе данных NSP. Информация об уязвимости также обновляется в кэше, поддерживаемом клиентом Alert Manager. Таким образом все компьютеры, на которых открыт Alert Manager, могут видеть последние запущенные сканирования по требованию.

Автоматическое или ручное импортирование отчетов Foundstone. Отчет об уязвимости может быть импортирован из базы данных Foundstone посредством Foundstone Scheduler в Network Security Platform. Отчеты можно планировать на ежедневной или еженедельной основе. Импортированная информация об уязвимости будет храниться в базе данных NSP и, кроме того, обновляться в кэш-памяти, используемой для анализа релевантности атак.

Вы можете вручную импортировать отчеты из Foundstone и сохранять их на локальной машине. Клиент NSP передает импортированные данные об уязвимости в модуль оценки уязвимости сервера NSP. Эта информация обрабатывается и хранится в базе данных NSP в формате Network Security Platform.

Анализ релевантности атак. Импортировав отчеты об уязвимости в базу данных Network Security Platform (NSP), можно определить релевантность уязвимости к предупреждениям в реальном времени.

Интегрирование с NAC: проверка после входа

McAfee NAC обнаруживает и оценивает системы, пытающиеся войти в вашу сеть, и перед тем как предоставить им доступ, может применить к системам проверку соответствия политике. Однако, безопасность сети не будет полной, если выполнять лишь проверку до входа. Для полноты и постоянства безопасности сети необходима также эффективная проверка после входа, например, с помощью Network Security Platform. Network Security Platform может в реальном времени предупредить вас об угрозах после входа и попытках действий эксплойта, например, системы, генерирующей вредоносный трафик. Для обезвреживания системы-нарушителя вы можете объединить усилия McAfee NAC и Network Security Platform (NSP). Например, при помощи NSP вы можете поместить систему в карантин и перенаправить весь HTTP-трафик системы на восстановительный портал до окончания восстановления.

Как это работает?

Шаг 1: Определяются системные политики соответствия и политики Network IPS.

Шаг 2: Датчик Network Security Platform обнаруживает аномальный трафик или вредоносную деятельность со стороны узла с подозрительным поведением.

Шаги 3 и 4: Network Security Platform блокирует атаку и либо сообщает MNAC, если узел контролируемый, либо, в случае неконтролируемого узла, помещает источник атаки в карантин при помощи функции «карантин».

Шаг 5: Опять же, в случае контролируемого узла, источник отправляется на автоматическое восстановление, неконтролируемый узел перенаправляется на портал восстановления.

Уверенность в обеспечении безопасности в реальном времени

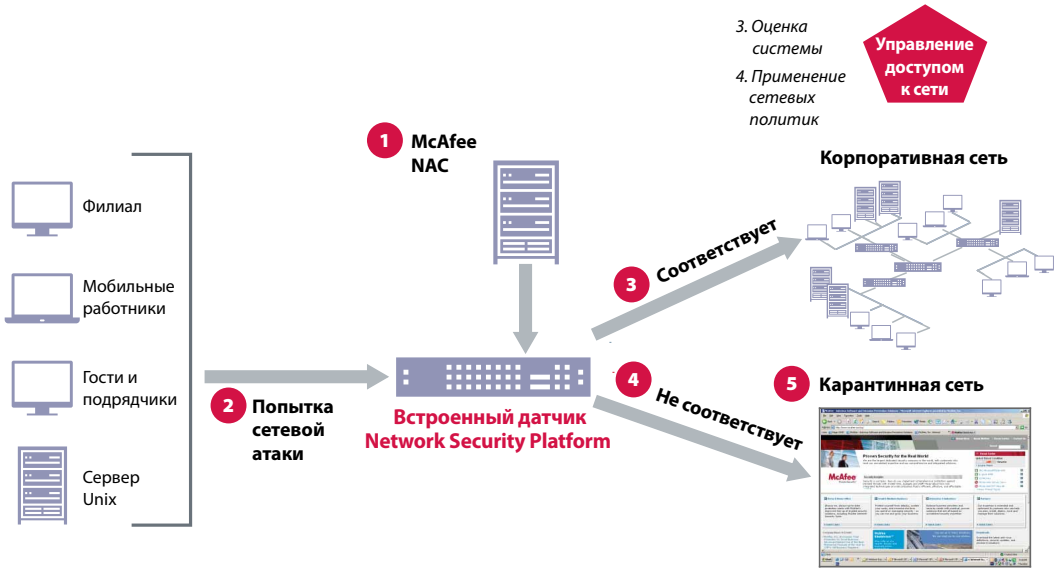
Интеллектуальная интеграция защиты сети и системы обеспечивает безопасность в реальном времени, которая не только автоматизирована, но и позволяет выполнять дальнейшие действия. С помощью одного щелчка мыши вы получаете интеллектуальную систему предотвращения вторжений, предоставляющую по запросу критическую информацию об узлах, наиболее важных вторжениях на узел и атаках шпионских программ, а также точное определение релевантности угрозы и риска. Решение реального времени для обеспечения защиты позволяет принимать решения относительно безопасности в реальном времени, обеспечивая:

McAfee

- Меньше времени на обеспечение защиты с помощью IPS с информацией о системе посредством интеграции с ePO
- Меньше времени на обеспечение доверия с помощью IPS в реальном времени с информацией о рисках посредством интеграции проверки уязвимости Foundstone
- Полная и постоянная безопасность сети с контролем до и после входа посредством интеграции с NAC

Традиционные системы предотвращения вторжений (IPS) являются решениями для конечных точек, часто дающими ложные положительные результаты и огромные журналы предупреждений. Свойственный им недостаток координации приводит к трате драгоценного времени на резервные процессы управления. Многие решения на базе ПК не масштабируются при атаке. Лишь некоторые из них предлагают контроль для уменьшения давления за счет установки «заплат».

Только Network Security Platform сочетает инфраструктуру сетевой и системной безопасности для упреждающей защиты в масштабах предприятия. Такая защита значительно точнее и эффективнее, чем традиционные точечные продукты. Можно управлять рисками и добиваться соответствия требованиям безопасности с меньшими усилиями. Интеллектуальная безопасность и надежные платформы сетевого класса Network Security Platform обеспечивают полную уверенность в безопасности.



1	2	3	4	5
Определение Определяются системные политики соответствия требованиям и политики Network IPS	**Обнаружение** Датчик Network Security Platform обнаруживает сетевой трафик от «узла с подозрительным поведением»	**Оценка** Network Security Platform блокирует атаки и с помощью базы данных MNAC определяет, является ли устройство контролируемым или неконтролируемым	**Применение политики** Network Security Platform отправляет неконтролируемый инфицированный узел в карантин согласно установленным политикам IPS	**Исправление** Система, помещенная в карантин, направляется в портал исправления для неконтролируемых систем

Интеграция McAfee NAC и Network Security Platform — Проверка после входа

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru