ЛИСТ ДАННЫХ

McAfee Virtual Network Security Platform

Комплексная технология обнаружения угроз в облачных сетях

McAfee® Virtual Network Security Platform представляет собой полноценную систему предотвращения сетевых угроз и вторжений (IPS), созданную с учетом уникальных особенностей частных и гибридных облаков. Платформа обнаруживает и блокирует изощренные угрозы в облачных архитектурах, отличаясь при этом точностью и простотой работы, что дает организациям возможность восстановить требуемый уровень нормативно-правового соответствия и уверенно перейти к использованию облачных технологий. Платформа включает в себя такие передовые технологии, как обнаружение угроз без использования сигнатур, встроенная эмуляция файлов, установка исправлений уязвимостей на основе сигнатур, поддержка Amazon Web Services (AWS) и виртуализации сети. Оптимизированные процессы, большое количество средств интеграции и упрощенный порядок лицензирования позволяют организациям легко управлять средствами защиты и масштабировать их в самых сложных облачных архитектурах.

Комплексное решение для защиты публичных облаков с использованием передовых технологий ИБ

Преимущество использования публичных облаков заключается в их удобстве, экономии средств и возможности перевести все расходы на инфраструктуру в операционные затраты. Вместе с тем, при использовании публичных облаков возникает новый уровень риска: наличие любой уязвимости в общедоступном программном обеспечении может привести к тому, что злоумышленник сможет проникнуть в облако и украсть конфиденциальную информацию, или к тому, что другие пользователи той же службы случайно получат доступ к данным клиентов. McAfee Virtual Network Security Platform поддерживает крупнейшую на сегодняшний день публичную облачную службу — AWS, обеспечивая полный сбор информации и о данных, проходящих

Ключевые преимущества

Беспрецедентная эффективность предотвращения сложных угроз

- Усовершенствованный механизм анализа вредоносных программ без использования сигнатур
- Защита от запуска межсайтовых сценариев и внедрения SQL-кода
- Эффективное обнаружение бот-сетей, обратных вызовов и вредоносных программ
- Поведенческий анализ и защита от атак типа «распределенный отказ в обслуживании» (DDoS)
- Интеграция с McAfee Advanced Threat Defense
- Развертывание систем предотвращения (IPS) и обнаружения (IDS) вторжений
- Решение по обеспечению непрерывной защиты McAfee Virtual Network Security Platform для VMware ESX

через интернет-шлюз, и о том, что происходит в межузловом трафике. Используя платформу IPS, позволяющую осуществлять по-настоящему эффективную проверку межузлового трафика, вы сможете восстановить требуемый уровень сбора информации об угрозах и нормативно-правового соответствия средств защиты в публичных облачных архитектурах.

Защита виртуализированных сред

В настоящее время в корпоративной среде наблюдается стремительный переход к использованию виртуализированной ИТ-инфраструктуры (частных и публичных облаков), позволяющей размещать на физических серверах сразу несколько разных виртуальных машин и даже целые виртуализированные рабочие нагрузки. Коммуникация между виртуальными машинами и необходимость мгновенно осуществлять миграцию, репликацию и резервное копирование этих рабочих нагрузок приводят к резкому увеличению объема межузлового трафика внутри частных и публичных облаков и программно определяемых ЦОД. А достигаемая благодаря виртуализации сети гибкость делает эти растущие потоки трафика динамичными и непредсказуемыми. Поэтому решения для защиты виртуализированных сред должны отличаться гибкостью и масштабируемостью, а также, что еще более важно, беспрепятственно взаимодействовать с платформами для развертывания программно определяемых сетей (SDN), обеспечивающими координацию этих зачастую недолговечных виртуальных машин и рабочих нагрузок.

Повышение динамичности в частных облаках

Платформа McAfee Virtual Network Security Platform, разработанная специально для защиты виртуализированных сред, беспрепятственно интегрируется с широко используемыми платформами для создания частных облаков, включая VMware NSX, и со средами для развертывания программно определяемых сетей (SDN) на базе OpenStack. Более того, McAfee Virtual Network Security Platform является единственной специализированной виртуальной IPS, сертифицированной для работы с VMware NSX. В виртуализированных средах микросегментация виртуальных машин и глубокая проверка межузлового трафика осуществляются непрерывно и автоматически даже в условиях быстрого создания, миграции и удаления рабочих нагрузок.

Беспрецедентный уровень предотвращения угроз

В основе McAfee Virtual Network Security Platform лежит архитектура следующего поколения, предназначенная для проведения глубокой проверки трафика в виртуальных сетях. Сочетание разных передовых методов проверки позволяет обнаруживать и предотвращать как известные атаки, так и атаки «нулевого дня». К этим методам относятся анализ трафика по всем протоколам, анализ репутации угроз, анализ поведения, расширенный анализ вредоносных программ и др.

Ни одна отдельно взятая технология обнаружения вредоносных программ не в состоянии предотвратить все возможные атаки.

Архитектура с поддержкой облачных технологий

- Одна лицензия позволяет распределять пропускную способность между публичными и частными облаками в любом их сочетании.
- Инновационный подход к проверке трафика AWS обеспечивает по-настоящему эффективную защиту межузлового трафика в публичном облаке.
- Поддержка координации со средами SDN на базе VMware NSX и OpenStack позволяет автоматизировать микросегментацию и проверку трафика между рабочими нагрузками в частных облаках.
- Панель мониторинга с возможностью мониторинга виртуальных машин и функцией принудительной отправки в карантин, активируемой при интеграции с VMware.
- Единая централизованная консоль управления для физических и виртуальных датчиков, развернутых локально и в облаке.

Интеллектуальное управление безопасностью

- Управление локальными и облачными датчиками, осуществляемое с единой консоли

Именно поэтому в McAfee Virtual Network Security Platform включено несколько разных модулей обнаружения угроз (с использованием и без использования сигнатур), дающих организациям возможность защитить свои облака от разрушительного воздействия нежелательных вредоносных программ. Платформа позволяет использовать множество технологий проверки трафика: встроенную эмуляцию веб-обозревателя, JavaScript и файлов Adobe; обнаружение бот-сетей и обратных вызовов из вредоносных программ; обнаружение DDoS-атак с помощью поведенческого анализа, а также защиту от сложных атак, проводимых путем запуска межсайтовых сценариев, внедрения SQL-кода и др. Кроме того, благодаря интеграции с решением McAfee Advanced Threat Defense, проводящим глубокий поведенческий анализ направляемых в него файлов, платформа McAfee Virtual Network Security Platform может также обнаруживать и блокировать тщательнейшим образом замаскированные и скрытые файлы. Благодаря сочетанию средств глубокого статического анализа кода и функций динамического анализа вредоносного ПО («в песочнице») с методами машинного обучения McAfee Advanced Threat Defense обеспечивает более высокую точность обнаружения угроз «нулевого дня», в том числе тех, в которых используются методы обхода защиты и программы-вымогатели.

Совместное использование лицензии в облаке

Сегодня многие предприятия, которым нужно обеспечить поддержку устаревших приложений, уменьшить зависимость от одного поставщика, обеспечить отказоустойчивость систем или сократить затраты, распределяют свои ИТ-ресурсы и инфраструктуру по различным облакам и платформам. Лицензирование защитных решений для виртуализированных сред может оказаться довольно сложным и дорогим делом, поскольку большинство поставщиков требует приобретения отдельных лицензий для разных частных и публичных облаков и разных платформ SDN.

Чтобы упростить порядок лицензирования и предоставить клиентам возможность сократить затраты, McAfee внедрила новую концепцию совместного использования лицензии в облаке, позволяющую клиентам использовать пропускную способность и лицензию McAfee Virtual Network Security Platform с любым сочетанием публичных и частных облачных платформ. Кроме того, концепция совместного использования лицензии в облаке способствует повышению уровня безопасности, поскольку дает администраторам возможность быстро обеспечивать защиту межузлового трафика и микросегментацию виртуальных рабочих нагрузок независимо от их местонахождения, при этом минуя долгую процедуру материально-технического снабжения.

Оптимизация рабочих процессов и аналитики

Вы сможете легко обнаруживать и блокировать самые изощренные угрозы. McAfee Virtual Network Security Platform включает в себя средства расширенного анализа и средства интеграции с дополнительными защитными решениями, что делает эту платформу для обнаружения и устранения угроз по-настоящему комплексной и интегрированной.

- Интеллектуальная корреляция и приоритизация предупреждений
- Выверенные панели для расследования вредоносных программ
- Рабочие процессы для расследования инцидентов, не требующие дополнительной настройки
- Масштабируемые функции управления через веб-консоль

Видимость и контроль

- Идентификация приложений
- Идентификация пользователей
- Идентификация устройств
- Состояние безопасности всех виртуальных машин в AWS

Современные угрозы могут генерировать такое большое количество предупреждений, что оператор системы безопасности быстро оказывается не в состоянии их приоритизировать и отслеживать. Но если вовремя не разобраться что к чему, то можно не заметить серьезных угроз безопасности. McAfee Virtual Network Security Platform содержит готовые средства расширенного анализа и наглядные рабочие процессы, позволяющие сводить разные предупреждения IPS в одно-единственное наглядное событие. Данный механизм помогает администраторам быстро отсеивать ненужное и добираться до важной информации, позволяющей принимать конкретные меры реагирования.

Централизованное управление в реальном времени данными, поступающими в реальном времени

Используя одно-единственное аппаратное устройство McAfee Network Security Manager, вы сможете с непревзойденной легкостью осуществлять централизованное управление всей системой через специальный веб-интерфейс. Консоль управления, отвечающая всем современным стандартам, и усовершенствованный графический интерфейс позволяют уверенно работать с данными, поступающими в режиме реального времени. Наличие единой консоли дает возможность легко осуществлять управление, настройку и мониторинг всех виртуальных и физических устройств McAfee Network Security Platform и устройств McAfee Network Threat Behavior Analysis во всех традиционных, облачных частных и облачных публичных ресурсах. Интуитивно понятный веб-интерфейс дает возможность проводить развертывания любого масштаба, от отдельных устройств до широко распределенных критически важных кластеров. McAfee Network Security Manager может быть также развернут как виртуальный экземпляр на серверах VMware ESX и в AWS.

Высокий уровень доступности и аварийное восстановление

McAfee Network Security Manager осуществляет управление контроллерами и назначает одному активный режим, а другому — режим ожидания. Когда активный контроллер становится недоступным, контроллер, находившийся в режиме ожидания, переходит в активный режим. Таким образом, благодаря механизму перехода на другой ресурс при сбое, когда один из контроллеров всегда является активным и доступным, обеспечивается высокий уровень доступности контроллера (англ. high availability, сокращенно HA) для развертывания в AWS. Кроме того, в режиме ожидания McAfee Network Security Manager обеспечивает аварийное восстановление для сред AWS.

McAfee Virtual Network Security Platform обеспечивает высокий уровень доступности с диспетчером аварийного восстановления (англ. manager disaster recovery, сокращенно MDR), высокий уровень доступности (HA) контроллера и функции автоматического масштабирования виртуальных датчиков IPS. Это позволяет гарантировать непрерывную и бесперебойную работу McAfee Virtual Network Security Platform.

Решение MDR предусматривает функцию второго диспетчера, который активируется в случае сбоя первого менеджера. Два контроллера высокого уровня доступности гарантируют, что один из них всегда активен и доступен, таким образом исключаются сбои в работе сети. Функция автоматического масштабирования виртуальных датчиков IPS создает новый виртуальный датчик IPS в случае сбоя какого-либо экземпляра датчика. Это выполняет функцию распределения нагрузки в случае увеличения сетевого трафика.

Централизованная архитектура защиты от угроз безопасности

Изощренные атаки не признают границ между отдельными продуктами и используют все бреши в инфраструктуре, особенно если речь идет об инфраструктуре безопасности. McAfee Virtual Network Security Platform — единственная система IPS, способная интегрироваться с разными защитными продуктами и использовать имеющиеся данные и рабочие процессы для устранения брешей. Использование платформы способствует повышению отдачи от инвестиций и снижению совокупной стоимости владения. Платформа включает в себя средства интеграции со следующими защитными продуктами:

- **Программное обеспечение McAfee ePolicy Orchestrator® (McAfee ePO™):** полный сбор информации о происходящем на конечных точках по всем событиям и предупреждениям IPS
- **McAfee Endpoint Intelligence Agent:** совмещение сетевой информации с информацией, поступающей с конечных точек, для остановки утечек данных
- **McAfee Enterprise Security Manager:** обмен подробными данными и помещение в карантин в ответ на предупреждения IPS
- **McAfee Threat Intelligence Exchange:** обмен информацией между устройствами разных типов
- **McAfee Global Threat Intelligence:** крупнейшая и самая активная служба оценки репутации в мире
- **McAfee Network Threat Behavior Analysis:** сбор информации о происходящем в масштабе всей сети
- **McAfee Virtual Advanced Threat Defense**
- **McAfee Cloud Threat Detection**
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE)**
- **Сторонние сканеры уязвимостей:** анализ узла и анализ рисков для конечных точек

Дополнительные функции

Дополнительные средства предотвращения угроз

- McAfee Gateway Anti-Malware для эмуляции поведения вредоносных программ
- Модуль эмуляции JavaScript в PDF (упрощенная «песочница»)
- Модуль поведенческого анализа Adobe Flash
- Защита от динамических техник обхода

Защита от бот-сетей и обратных вызовов с передачей вредоносного кода

- Обнаружение обратных вызовов fast flux серверов доменных имен (DNS)/алгоритмов генерации доменных имен (DGA)
- Подмена доменов с помощью DNS-сервера (sinkholing)
- Эвристическое распознавание ботов
- Сопоставление большого количества разных атак
- База данных о центрах управления бот-сетями

Дополнительные средства предотвращения вторжений

- Дефрагментация IP-пакетов и восстановление TCP-потоков
- Поддержка сигнатур McAfee, сигнатур пользователей и сигнатур из открытых источников
- Помещение узлов в карантин и ограничение числа подключений
- Проверка виртуальных сред
- Предотвращение атак по типу отказа в обслуживании и распределенного отказа в обслуживании (DoS и DDoS)
- Обнаружение угроз пороговым и эвристическим методами
- Ограничение числа подключений на узлах
- Обнаружение угроз путем самообучения на основе профилей

McAfee Global Threat Intelligence

- Репутация файлов
- Репутация IP-адресов
- Ограничение доступа на основе местонахождения
- Управление доступом на основе IP-адресов

ЛИСТ ДАННЫХ

	Датчик типа 1	Датчик типа 2	Датчик типа 3
Платформа	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 NSX 6.3 AWS
Модель виртуальных датчиков IPS	IPS-VM100	IPS-VM600	IPS-VM100-VSS[1]
Тип развертывания виртуальной системы IPS	Автономный	Автономный	Распределенный
Поддержка VMware NSX	Нет	Нет	Да
Поддержка AWS	Нет	Нет	Да
Кол-во логических ядер ЦП[2]	3	4	3
Объем ОЗУ[3]	4 ГБ	6 ТБ	5 ГБ
Спецификации для виртуальных датчиков			
Максимальная пропускная способность[4]	до 500 Мбит/с	до 1 Гбит/с	до 500 Мбит/с
Кол-во параллельных подключений	200 000	600 000	200 000
Кол-во новых соединений в секунду	6 000	20 000	6 000
Кол-во потоков UDP	39 168	254 208	39 168
Кол-во пар портов для мониторинга	2	3	1[5]
Кол-во виртуальных интерфейсов (VIDS) на датчик	32	100	32
Кол-во профилей DoS	100	300	100
Порт управления	Да	Да	Да
Ответный порт	Да	Да	Нет
Режимы развертывания	Проверка трафика между виртуальными машинами, между физическими машинами и между физическими и виртуальными, а также трафика на портах SPAN		Линейная проверка в VMware NSX

1. Для использования только в средах VMware NSX в качестве службы, внедренной в виртуальную среду VMware.
2. Требования к ресурсам виртуальной среды могут измениться в последующих выпусках. Дополнительные сведения см. в документации к конкретному выпуску.
3. Там же.
4. Измерение проводилось с использованием пакетов UDP размером 1 518 байт в оптимальных условиях.
5. Виртуальное представление входа и выхода. Проверка тесно привязана к VMware NSX на уровне ядра.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru