McAfee Virtual Network Security Platform

Комплексная технология обнаружения и предотвращения вторжений в облачных сетях

McAfee® Virtual Network Security Platform (McAfee® vNSP) представляет собой полноценную систему обнаружения и предотвращения сетевых угроз и вторжений (IPS), созданную с учетом уникальных особенностей частного и публичного облака. Она отличается высокой скоростью, точностью и простотой обнаружения и блокирования изощренных угроз в облачных архитектурах, что дает организациям возможность обеспечить надежную защиту рабочих нагрузок и восстановить требуемый уровень нормативно-правового соответствия. В ней используются такие передовые технологии, как бессигнатурное обнаружение угроз, встроенная эмуляция, установка исправлений с использованием сигнатур. Наличие оптимизированных рабочих процессов, автомасштабирования, гибких возможностей интеграции и упрощенной модели лицензирования облегчает организациям задачу управления защитой и ее масштабирования для удовлетворения текущих и будущих потребностей.

Комплексная защита публичных облаков

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 того же сервиса случайно получат доступ к данным клиентов. McAfee Virtual Network Security Platform поддерживает крупнейшие на сегодняшний день публичные облачные сервисы — Amazon Web Services (AWS), Microsoft Azure и Oracle Cloud Infrastructure (OCI), обеспечивая полный сбор информации об угрозах и защиту данных, проходящих через интернет-шлюз и передающихся в межузловом трафике.

Ключевые преимущества

- Полная защита частных и публичных облаков (AWS, Azure и OCI)
- Встроенные системы предотвращения вторжений (IPS)/обнаружения вторжений (IDS) с выбором соответствующего режима работы
- По-настоящему эффективная защита межузлового трафика
- Унифицированные политики и процессы управления
- Передовые технологии проверки обеспечивают защиту от известных и неизвестных угроз
- Высокий уровень отказоустойчивости, средства аварийного восстановления и механизм распределения нагрузки для повышения производительности

Подписаться

Защита виртуальных 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 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 центров обработки данных. 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.

Динамичность в частном облаке

Для защиты виртуальных сетей в инфраструктуре частного облака платформу McAfee Virtual Network Security Platform можно развертывать в виде виртуального устройства на сервере VMware ESX. Виртуальное устройство, развертываемое как образ в формате OVF (Open Virtualization Format — открытый формат виртуализации), поможет осуществлять проверку трафика между виртуальными машинами на конкретном узле ESX, а также на различных узлах ESX и в физических сетях.

Средства предотвращения сложных угроз

В основе McAfee Virtual Network Security Platform лежит архитектура следующего поколения, предназначенная для проведения глубокой проверки трафика в виртуальных сетях. Сочетание различных передовых методов проверки позволяет обнаруживать и предотвращать как известные атаки, так и неизвестные 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. Именно поэтому в McAfee Virtual Network Security Platform включено несколько различных модулей обнаружения угроз (с использованием и без использования сигнатур), дающих организациям возможность защитить свои облака от разрушительного воздействия нежелательных вредоносных программ. В платформе используются различные технологии проверки трафика: встроенная эмуляция веб-обозревателя, JavaScript и файлов Adobe; обнаружение бот-сетей и обратных вызовов из вредоносных программ; обнаружение DDoS-атак с помощью поведенческого анализа, а также защита от сложных атак, проводимых путем запуска межсайтовых сценариев, внедрения SQL-кода и др.

Кроме того, благодаря интеграции с решением McAfee® Advanced Threat Defense, проводящим поведенческий анализ направляемых в него

Ключевые преимущества (продолжение)

- Модель совместного использования лицензии в облаке позволяет работать с разными сочетаниями публичных и частных облаков
- Интеграция с набором решений McAfee для защиты на всем пути от устройств к облаку
- Имеется в AWS Marketplace
- Имеется в Azure Marketplace

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 при обнаружении угроз «нулевого дня», в том числе тех, в которых используются методы обхода защиты и программы-вымогатели. Кроме того, McAfee обеспечивает встроенную поддержку сигнатур Snort для обнаружения вредоносных программ и защиты от них.

Гибкий механизм совместного использования лицензий в облаке

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 процессом, поскольку большинство поставщиков требует приобретения отдельных лицензий для различных частных и публичных облаков.

За счет предложенной компанией McAfee модели совместного использования лицензий в облаке упрощается порядок лицензирования и снижаются затраты, что позволяет организациям использовать лицензии McAfee Virtual Network Security Platform с любым сочетанием публичных и частных облачных платформ. Модель совместного использования лицензий в облаке предоставляет бóльшую свободу выбора и способствует повышению уровня безопасности, поскольку дает администраторам возможность быстро обеспечивать защиту межузлового трафика и микросегментацию виртуальных рабочих нагрузок независимо от их местонахождения, не тратя времени на сложные схемы лицензирования и долгие процессы материально-технического снабжения.

Оптимизация рабочих процессов и аналитики

Современные угрозы могут генерировать настолько большое количество предупреждений, что оператор системы безопасности быстро оказывается не в состоянии их приоритизировать и отслеживать. Если реагировать слишком медленно, то можно пропустить и не заметить серьезные угрозы безопасности. McAfee Virtual Network Security Platform включает в себя средства расширенного анализа и рабочие процессы, сводящие большое количество разных предупреждений IPS в одно-единственное событие, позволяющее администраторам быстро выявлять важную информацию. А интеграция с дополнительными защитными решениями McAfee делает платформу для обнаружения и устранения сетевых угроз по-настоящему комплексной.

Унифицированные политики и процессы управления

Решение McAfee® Network Security Manager может быть развернуто в виде виртуального экземпляра на серверах VMware ESX и в средах AWS, Azure или OCI. Благодаря этому администраторы систем ИБ смогут согласованно расширять зону действия локального профиля безопасности до гибридных центров обработки данных по мере переноса рабочих

нагрузок на облачные платформы и управлять ими, используя унифицированную консоль управления и унифицированные рабочие процессы. McAfee Virtual Network Security Platform поддерживает AWS Identity and Access Management (IAM), что дает администраторам возможность легко и безопасно управлять доступом к сервисам и ресурсам AWS исходя из разрешений, назначенных тем или иным пользователям и группам.

Высокий уровень отказоустойчивости, средства аварийного восстановления и механизм распределения нагрузки

McAfee Virtual Network Security Platform в автоматическом режиме обеспечивает непрерывный контроль, защиту и быстродействие за счет применения различных методов. Высокий уровень доступности обеспечивается путем упреждающего мониторинга среды с помощью McAfee Network Security Manager. Например, когда активный контроллер становится недоступным, запускается новый экземпляр контроллера. Кроме того, для обеспечения аварийного восстановления в средах AWS, Azure и OCI можно развернуть McAfee Network Security Manager в режиме ожидания.

McAfee Virtual Network Security Platform также обеспечивает высокий уровень доступности датчиков IPS. Если датчик становится недоступным, функция автоматического масштабирования автоматически создает новый виртуальный датчик IPS, обеспечивая тем самым непрерывную защиту. А при увеличении объема сетевого трафика функция автоматической балансировки нагрузки на датчики оптимизирует быстродействие, причем развертывание дополнительных датчиков, необходимых для обеспечения требуемой пропускной способности, выполняется автоматически.

Встроенная безопасность

Изощренные атаки не признают границ между отдельными продуктами и не преминут воспользоваться любыми брешами в инфраструктуре, особенно брешами между продуктами безопасности. McAfee Virtual Network Security Platform — единственная система IPS, способная беспрепятственно интегрироваться с разными защитными продуктами и обеспечивать надежную защиту и повышение отдачи от инвестиций путем эффективного использования данных и рабочих процессов без привязки к какому-то одному решению. Интегрируется, среди прочего, со следующими решениям McAfee:

- **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 предотвращения 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:** обеспечивает углубленную проверку с целью обнаружения трудноуловимых угроз
- **McAfee® Management for Optimized Virtual Environments (McAfee® MOVE):** антивирусное решение для виртуальных сред
- **Сторонние сканеры уязвимостей:** анализ узла и анализ рисков для конечных точек

Дополнительные функции

Средства предотвращения сложных угроз

- Усовершенствованная защита от вредоносных программ
- Встроенная проверка входящего SSL-трафика
- Углубленная проверка файлов Microsoft Office
- Модуль эмуляции JavaScript в PDF (упрощенная «песочница»)
- Модуль поведенческого анализа Adobe Flash
- Усовершенствованная технология предотвращения попыток обхода системы защиты

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
- Командно-контрольная база данных

Усовершенствованная технология предотвращения вторжений

- IP-дефрагментация и потоковая перекомпоновка TCP
- Поддержка сигнатур, создаваемых McAfee, создаваемых пользователем и получаемых из открытых источников
- Помещение узлов в карантин и ограничение числа подключений
- Проверка виртуальных сред
- Предотвращение атак типа «отказ в обслуживании» (DoS) и «распределенный отказ в обслуживании» (DDoS)
- Белые/черные списки для поддержки файлов в формате Structured Threat Information eXpression — STIX
- Обнаружение угроз пороговым и эвристическим методом
- Ограничение подключений по узлам
- Встроенная поддержка сигнатур Snort
- Обнаружение угроз путем самообучения на основе профилей

McAfee Global Threat Intelligence

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

	Датчик типа 1	Датчик типа 2
Платформа	VMware ESX	AWS Azure OCI
Модель виртуальных датчиков IPS	IPS-VM600	IPS-VM600-VSS
Тип развертывания виртуальной системы IPS	Автономный	Распределенный
Поддержка AWS	Нет	Да
Поддержка Azure	Нет	Да
Поддержка OCI	Нет	Да
Кол-во логических ядер ЦП	4	4
Объем ОЗУ	8 ГБ	8 ГБ
Хранение данных	40 ГБ	40 ГБ
Спецификации для виртуальных датчиков		
Максимальная пропускная способность	до 1 Гбит/с	до 1 Гбит/с
Кол-во пар портов для мониторинга	3	1 (порт для мониторинга, не пара портов)
Кол-во виртуальных интерфейсов (VIDS) на датчик	100	100
Кол-во профилей DoS	300	300
Порт управления	Да	Да
Ответный порт	Нет	Нет
Режимы развертывания	Проверка трафика между виртуальными машинами, между физическими машинами и между физическими и виртуальными машинами, а также трафика на портах SPAN и линейная проверка портов	

Дополнительная информация

- Защита виртуальных сетей на базе Amazon Web Services
- Защита виртуальных сетей на базе Microsoft Azure

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