McAfee Network Security Platform

Платформа для комплексной и интеллектуальной защиты от сложных угроз

McAfee® Network Security Platform представляет собой систему обнаружения и предотвращения вторжений (IPS) следующего поколения, выявляющую и блокирующую изощренные вредоносные программы в масштабах всей сети. Она не ограничивается простым сопоставлением наблюдаемых явлений с имеющимися образцами, а использует передовые методы обнаружения угроз и эмуляции поведения, что позволяет обеспечивать защиту от скрытых атак с высочайшей степенью точности. Платформа способна обрабатывать данные со скоростью свыше 30 Гбит/с при использовании одного устройства, а при объединении в стек — до 100 Гбит/с. Именно такие скорости необходимы для защиты крупных сетей. Комплексный набор решений McAfee позволяет оптимизировать операции по обеспечению безопасности, поскольку информация об угрозах, получаемая в режиме реального времени от службы McAfee® Global Threat Intelligence, дополняется подробными контекстными данными о пользователях, устройствах и приложениях. Такой подход позволяет быстро и точно реагировать на сетевые атаки.

Ключевые преимущества

- Быстрое обнаружение и блокирование угроз, обеспечивающее защиту приложений и данных
- Высокоэффективное масштабируемое решение для динамических сред
- Централизованное управление с целью оптимизировать сбор информации и контроль
- Передовые методы обнаружения угроз, в том числе анализ вредоносных программ без использования сигнатур

Защита от современных скрытых угроз

Одним из результатов цифровизации стали кардинальные изменения в области информационной безопасности. Облачные службы, мобильные устройства и Интернет вещей создали новые уровни сетевых подключений, на которых не существует реальной границы или рубежа, которые можно было бы оборонять. Количество и степень серьезности рисков в одночасье выросли в геометрической прогрессии. Многие предприятия стали уделять внимание защите данных, в результате чего важнейшим условием защиты этих данных стало наличие надежной стратегии сетевой безопасности. Ваша сеть сталкивается с изощренными скрытыми атаками, не поддающимися обнаружению с помощью традиционных методов обнаружения атак, что подвергает ваши приложения и данные риску серьезных взломов и перебоев

Подписаться

в работе. К сожалению, большинству организаций не хватает финансовых и организационных ресурсов для внедрения и обслуживания того набора инструментов и технологий, который необходим для обеспечения адекватной защиты.

McAfee Network Security Platform сочетает в себе интеллектуальные средства предотвращения угроз и интуитивно понятные средства управления защитой, что дает возможность повысить точность обнаружения угроз и оптимизировать операции по обеспечению безопасности. Ни одна отдельно взятая технология обнаружения вредоносных программ не в состоянии предотвратить все возможные атаки. Именно поэтому в McAfee Network Security Platform включено несколько разных модулей обнаружения угроз с использованием и без использования сигнатур. Это дает организациям возможность защитить свои сети от разрушительного воздействия нежелательных вредоносных программ. Система осуществляет углубленную проверку сетевого трафика, используя сочетание различных передовых методов, таких как анализ трафика по всем протоколам, анализ репутации угроз, анализ поведения и расширенный анализ вредоносных программ. Это позволяет обнаруживать обратные вызовы с передачей вредоносного кода, атаки типа «отказ в обслуживании» (DoS), атаки «нулевого дня» и другие сложные угрозы, а также обеспечивать защиту от них.

Встроенная безопасность

Благодаря сочетанию средств глубокого статического анализа кода и функций динамического анализа вредоносного ПО («в песочнице») с методами машинного обучения, платформа McAfee Network Security Platform, интегрированная с McAfee® Advanced Threat Defense, обеспечивает обнаружение угроз «нулевого дня», в том числе тех, в которых используются методы обхода защиты и программы-вымогатели. McAfee Network Security Platform также использует информацию о репутации файлов, собираемую с помощью McAfee Global Threat Intelligence, и поддерживает интеграцию с программным обеспечением McAfee® ePolicy Orchestrator® и McAfee® Enterprise Security Manager, что дает возможность проводить сопоставление сетевых событий из всех значимых источников в режиме реального времени. В объединенном решении используются данные об устройствах, информация о пользователях, данные о степени защищенности конечных точек, результаты оценки уязвимости и другие подробные данные, помогающие организациям анализировать степень серьезности угрозы и факторы коммерческого риска.

Ключевые преимущества (продолжение)

- Расшифровка SSL с целью проверки входящего и исходящего сетевого трафика
- Высокий уровень доступности и аварийное восстановление
- Наличие виртуальных устройств
- Интеграция с набором решений McAfee для защиты на всем пути от устройств к облаку

Производительность и доступность

Воспользуйтесь обоими преимуществами McAfee Network Security Platform — безопасностью и высоким уровнем быстродействия. Платформа сочетает в себе средства однопроходной проверки трафика на основе протоколов со специальным аппаратным обеспечением операторского класса, что позволяет в реальных условиях осуществлять проверку трафика со скоростью свыше 100 Гбит в секунду. Эффективность ее архитектуры позволяет сохранять высокий уровень быстродействия независимо от настроек безопасности, в то время как у других систем IPS при использовании политик, ставящих безопасность выше быстродействия, сокращение пропускной способности может составить до 50 процентов.

Кроме того, McAfee Network Security Platform поддерживает режимы «активный–активный» и «активный–пассивный» с возможностью при сбое перейти на другой ресурс, сохраняя состояние соединений. Это дает вам возможность обеспечить соответствие требованиям, предъявляемым к высокой степени доступности соглашений об уровне обслуживания (SLAs), и в то же время избежать «узких мест», возникающих при использовании устройств с меньшим быстродействием или перегруженных автономных решений.

Масштабируемая аппаратная платформа обеспечивает защиту капиталовложений

Устройства McAfee серий NS7500 и NS9500 дают клиентам свободу действий: приобретая устройство для текущих нужд, клиенты получают возможность легко масштабировать его пропускную способность в соответствии со своими меняющимися потребностями, приобретая лицензии на ПО. Что касается устройства McAfee NS9500, то дополнительная мощность достигается путем соединения нескольких устройств McAfee NS9500.

Сбор информации и контроль

Принимая решения, касающиеся приложений и протоколов в своей сети, организация должна руководствоваться конкретной, надежной информацией. McAfee Network Security Platform является первой системой обнаружения и предотвращения вторжений, в которой средства предотвращения сложных угроз и средства сбора информации о приложениях сведены в единый модуль, позволяющий принимать обоснованные решения по обеспечению безопасности. Мы сопоставляем информацию об угрозах с данными об использовании приложений, включая информацию 7-го (прикладного) уровня о более 2 000 приложений и протоколов, что дает вам возможность с большей уверенностью принимать решения о том, какие приложения допускать к работе в вашей сети.

В дополнение к функции идентификации приложений McAfee Network Security Platform обеспечивает сбор информации о пользователях и устройствах. Функция обнаружения аномального сетевого поведения позволяет приоритизировать опасные узлы и опасных пользователей, в том числе активные бот-сети.

Интеллектуальное, масштабируемое управление безопасностью

Интеллектуальный механизм управления сетевой безопасностью позволяет получить максимальную отдачу от инвестиций в средства обеспечения безопасности. Количество аппаратных устройств сетевой защиты, которыми можно управлять с помощью веб-консоли McAfee Network Security Manager, составляет от двух до нескольких сотен. Интуитивно понятные рабочие процессы McAfee Network Security Manager, разработанные в соответствии с принципом «последовательного раскрытия», направляют внимание администраторов на важные предупреждения, а простые в использовании панели мониторинга автоматически определяют приоритеты событий исходя из степени серьезности предупреждения и значимости события.

Дополнительные функции

Средства предотвращения сложных угроз

- При помощи общего ключа на основе агента расшифровка входящего трафика с использованием протокола Secure Sockets Layer (SSL) поддерживает шифрование по алгоритму Диффи-Хеллмана (DH) и алгоритму Диффи-Хеллмана на эллиптических кривых (ECDH), не влияя на быстродействие датчика (заявка на патент для серии NS подана).
- Исходящая расшифровка SSL (серия NS)
- McAfee® Gateway Anti-Malware для эмуляции поведения вредоносных программ
- Модуль эмуляции JavaScript в PDF-файлах
- Модуль поведенческого анализа Adobe Flash
- Модуль глубокой проверки файлов Microsoft Office
- Усовершенствованная технология предотвращения попыток обхода системы защиты
- Анализ репутации мобильных угроз и облачных приложений

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

- Обнаружение обратных вызовов с использованием DNS Fast Flux и 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
- Встроенная поддержка сигнатур Snort (серия NS)
- Усовершенствованные списки разрешений и блокирований для поддержки файлов в формате Structured Threat Information eXpression — STIX (серия McAfee NS)

- Помещение узлов в карантин и ограничение числа подключений
- Проверка виртуальных сред
- Интеграция с McAfee Advanced Threat Defense
- Поддержка распаковки ответов HTTP

Средства предотвращения атак DoS и DDoS

- Обнаружение угроз пороговым и эвристическим методом
- Ограничение подключений по узлам
- Обнаружение угроз путем самообучения на основе профилей

McAfee Global Threat Intelligence

- Репутация файлов, IP-адресов и URL-адресов
- Репутация приложений и протоколов
- Геопозиционирование
- Технология списков разрешений на основе категорий, присваиваемых службой McAfee Global Threat Intelligence

Высокий уровень доступности

- Режимы «активный–активный» и «активный–пассивный» с возможностью при сбое перейти на другой ресурс, сохраняя состояние соединений
- Внешняя функция открытия при отказе (активная)
- Встроенная функция открытия при отказе

Поддержка туннелирования протоколов

- IPv6
- Туннели V4-in-V4, V4-in-V6, V6-in-V4 и V6-in-V6
- MPLS
- GRE
- Q-in-Q Double VLAN

McAfee® Network Security Manager

- Многоуровневое управление (до 1 000 датчиков)
- Аутентификация пользователей (Radius и LDAP)
- Автоматическая отработка отказа и отказовозвращение
- Аварийное восстановление критически важных данных конфигурации
- Централизованная и иерархическая структура управления политиками
- Подробная информация на панели памяти, распределение памяти по устройствам

Дополнительная информация

Более подробную информацию и варианты физических устройств см. в документе Технические характеристики McAfee Network Security Platform.

Подробнее о том, на что обращать внимание при выборе системы IDPS.

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