McAfee Network Security Platform

Беспрецедентно «умный» подход к сетевой безопасности

McAfee® Network Security Platform — это беспрецедентно «умное» решение, способное обнаруживать и блокировать изощренные угрозы в сети. Используя передовые методы обнаружения угроз и эмуляции поведения, оно выходит за рамки простого сопоставления кода с образцом и с высочайшей точностью нейтрализует скрытые атаки. Являясь аппаратной платформой следующего поколения, она способна с одним устройством обеспечивать скорость передачи данных свыше 40 Гбит/с, что позволяет удовлетворять потребности высокопроизводительных сетей. Концепция управления системой безопасности Security Connected позволяет оптимизировать операции по обеспечению безопасности благодаря использованию информации об угрозах, собираемой в режиме реального времени при помощи технологии McAfee Global Threat Intelligence (McAfee GTI), в сочетании с подробными контекстными данными о пользователях, устройствах и приложениях. Это дает возможность быстро и точно реагировать на сетевые атаки.

Ключевые преимущества

Беспрецедентное предотвращение сложных угроз

- Усовершенствованные функции анализа вредоносных программ без использования сигнатур
- Линейная эмуляция браузера и JavaScript
- Усовершенствованный механизм обнаружения бот-сетей и обратных вызовов с передачей вредоносного кода
- Поведенческий анализ и защита от DDoS-атак
- Интеграция с McAfee Advanced Threat Defense

Security Connected

- Обмен информацией об угрозах посредством McAfee Threat Intelligence Exchange (TIE) в режиме реального времени
- Получение контекстной информации с конечных точек посредством ePolicy Orchestrator® (McAfee ePO™)
- Сопоставление процессов на конечных точках посредством Endpoint Intelligence Agent

Защита от современных скрытых угроз безопасности

Ваша сеть сталкивается с изощренными скрытыми атаками, не поддающимися обнаружению с помощью традиционных методов обнаружения атак, что подвергает ее риску серьезных взломов и перебоев 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.

Платформа McAfee Network Security Platform — интегрированное решение, сочетающее в себе интеллектуальные средства предотвращения угроз и интуитивно понятные средства управления системой защиты, что дает возможность обнаруживать угрозы с большей точностью и оптимизировать операции по обеспечению безопасности. Оно обеспечивает лучшую в отрасли защиту от сложных вредоносных программ, обратных вызовов с передачей вредоносного кода, угроз «нулевого дня» и атак типа «отказ в обслуживании». Платформа Network Security Platform, с самого начала создававшаяся для интеграции в экосистему Security Connected, получает и использует данные о безопасности всех имеющихся в организации конечных точек, что помогает закрывать такие бреши в защите, которые зачастую невозможно обнаружить с помощью других защитных решений, по частям собранных из разных продуктов.

Беспрецедентный уровень предотвращения угроз

В основе McAfee Network Security Platform лежит следующее поколение архитектуры, предназначенной для проведения глубокой проверки сетевого трафика на скоростях, соответствующих пропускной способности канала. Используемая в ней комбинация передовых методов проверки позволяет обнаруживать и предотвращать как известные, так и еще неизвестные атаки в сети. К этим

intel Security

Ключевые преимущества (продолжение)

Security Connected (продолжение)

- Обмен данными и помещение объектов в карантин с помощью McAfee Enterprise Security Manager (SIEM)
- Анализ уязвимости узлов посредством McAfee Vulnerability Manager
- Предсказательная модель обнаружения вредоносных программ с помощью McAfee GTI

Производительность и доступность

- Архитектура следующего поколения
- Пропускная способность до 40 Гбит/с
- Непревзойденный уровень быстродействия при проведении проверок SSL
- Лидер отрасли по показателю надежности
- Доступность в режимах «активный–активный» и «активный–пассивный»

Интеллектуальное управление безопасностью

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

Информированность и контроль

- Идентификация приложений
- Идентификация пользователей
- Идентификация устройств

методам относятся анализ трафика по всем протоколам, анализ репутации угроз, анализ поведения, усовершенствованный анализ вредоносных программ и др.

Комплексная защита от вредоносных программ

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. К ним относятся метод анализа репутации файлов посредством McAfee GTI, метод глубокого анализа файлов на наличие JavaScript и передовой метод обнаружения вредоносных программ, в том числе вредоносных программ особого назначения и иных скрытых атак.

Security Connected

Получить необходимые вам данные стало просто как никогда. Продукты McAfee в режиме реального времени интегрируются с программным обеспечением McAfee ePO и с McAfee Enterprise Security Manager, что дает возможность проводить сопоставление сетевых событий из всех необходимых источников в режиме реального времени. Интеграция с программным обеспечением McAfee ePO и с решением McAfee Enterprise Security Manager дает платформе McAfee Network Security Platform возможность получать точное представление об угрозах в их отношении к устройствам и пользователям, а также о том, какие из угроз представляют наибольший риск для организации. В 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.

Производительность и масштабируемость

Воспользуйтесь обоими преимуществами — безопасностью и высоким уровнем быстродействия. McAfee Network Security Platform 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 40 Гбит в секунду на одном-единственном устройстве. Чрезвычайная эффективность ее архитектуры позволяет сохранять высокий уровень быстродействия независимо от настроек безопасности, в то время как у других систем предотвращения вторжений (IPS) при использовании политик, ставящих безопасность выше быстродействия, сокращение пропускной способности может составить до 50 процентов.

Информированность и контроль

При принятии решений, касающихся приложений и протоколов в вашей сети, вы сможете руководствоваться конкретной информацией. McAfee Network Security Platform является первой и единственной системой предотвращения вторжений, в которой передовые средства предотвращения угроз и сбора информации о приложениях совмещены в едином модуле, позволяющем принимать решения относительно обеспечения безопасности вашей сети. Мы сопоставляем информацию об угрозах с данными об использовании приложений, включая информацию 7-ого уровня о более чем 1 500 приложениях и протоколах, 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. А функция обнаружения аномального сетевого поведения позволяет приоритизировать сомнительные узлы и пользователей, включая активные бот-сети.

Интеллектуальное управление безопасностью

Система автоматического управления сетевой безопасностью позволяет получить максимальную отдачу от инвестиций в систему безопасности. Количество устройств сетевой защиты, которыми можно управлять с помощью веб-консоли McAfee Network Security Manager, составляет от двух до нескольких сотен. В McAfee Network Security Manager используются интуитивно понятные рабочие процессы, основанные на методе «последовательного раскрытия» и дающие администраторам возможность получать необходимые оповещения, а также простые в использовании панели

McAfee Network Security Platform помогает в следующих областях:

Устранение брешей в системе защиты
- Блокирование вредоносных действий в сети
- Предотвращение скрытых атак
- Обнаружение сложных вредоносных программ

Упрощение процесса управления
- Автоматическая приоритизация событий
- Оптимизация процессов по расследованию инцидентов
- Устранение работы по настройке оборудования

Адаптация к сети
- Поддержка 1-гигабитного, 10-гигабитного и 40-гигабитного Ethernet
- Макс. скорость 40 Гбит/с
- Доступность в режимах «активный–активный» и «активный–пассивный»

мониторинга, автоматически определяющие приоритеты событий на основе их серьезности и значимости. McAfee Network Security Platform интегрируется с программным обеспечением McAfee ePO, что позволяет вам иметь единую консоль для просмотра информации о рисках и нормативно-правовом соответствии в масштабах всей компании. Такая информация включает актуальные данные о степени защищенности инфраструктуры компании, получаемые путем оценки обнаруженных системных уязвимостей, имеющихся средств сетевой защиты и уровней безопасности конечных точек.

Дополнительные функции

Предотвращение сложных угроз
- Модуль McAfee Gateway Anti-Malware (GAM) для эмуляции поведения
- Модуль эмуляции JavaScript в PDF-файлах
- Модуль поведенческого анализа Adobe Flash
- Защита от динамических техник обхода
- Анализ репутации мобильных угроз и облачных приложений

Защита от бот-сетей и обратных вызовов с передачей вредоносного кода
- Обнаружение обратных вызовов при использовании DNS Fast Flux и алгоритмов генерации доменных имен (DGA)
- Подмена доменов с помощью DNS-сервера
- Эвристическое распознавание ботов
- Сопоставление большого количества разных атак
- База данных центров управления бот-сетями

Передовые средства 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
- Контроль виртуальных сред

Средства предупреждения атак DoS и DDoS
- Обнаружение угроз пороговым и эвристическим методом
- Ограничение количества подключений на узлах
- Обнаружение угроз путем самообучения на основе профиля

McAfee GTI
- Репутация файлов
- Репутация IP-адресов
- Географическое местонахождение

Высокая отказоустойчивость
- 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 протокола
- 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
- Многоуровневая архитектура управления, рассчитанная на 1 000 датчиков
- Аутентификация пользователя (Radius и LDAP)
- Автоматическая отработка отказа и отказовозвращение
- Аварийное восстановление критически важных данных конфигурации
- Централизованная и иерархическая структура управления политиками

Спецификации McAfee Network Security Platform

	Аппаратное обеспечение следующего поколения		
Компоненты аппаратного обеспечения датчика	 **NS9300**	 **NS9200**	 **NS9100**
Производительность			
Реальная пропускная способность	40 Гбит/с	20 Гбит/с	10 Гбит/с
Максимальная пропускная способность (UDP, пакеты по 1 512 байт)	До 70 Гбит/с	До 35 Гбит/с	До 30 Гбит/с
Максимальное кол-во параллельных подключений	32 000 000	16 000 000	13 000 000
Кол-во соединений по TCP в секунду	1 150 000	575 000	450 000
Кол-во соединений по HTTP в секунду	750 000	375 000	260 000
Пропускная способность при использовании SSL (доля SSL-трафика: 10 %)	40 Гбит/с	20 Гбит/с	10 Гбит/с
Максимальное кол-во потоков SSL	3 200 000	1 600 000	1 200 000
Кол-во импортированных ключей SSL	1 024	1 024	1 024
Типичная задержка	Менее 100 мкс	Менее 100 мкс	Менее 100 мкс
Кол-во виртуальных систем предотвращения вторжений (IPS)	1 000	1 000	1 000
Максимальное кол-во профилей DoS	5 000	5 000	5 000
Кол-во правил ACL	20 000	20 000	20 000
Порты			
Фиксированные порты Gigabit Ethernet, медные (внутренние, открыты при отказе)	16	8	8
Фиксированные порты 10 GigE/1 GigE (SFP+)	—	—	—
Постоянные порты 40-Gigabit Ethernet	—	2	2
Гнезда для сетевых плат ввода-вывода	4	2	2
Сетевые платы ввода-вывода (4 варианта)	4 порта (QSFP+) 40 GigE, 2 порта (QSFP+) 40 GigE, 8 портов (SFP+/SFP) 10 GigE/1 GigE или 6 портов (RJ45) 1 GigE (с внутренней функцией открытия при отказе)	4 порта (QSFP+) 40 GigE, 2 порта (QSFP+) 40 GigE, 8 портов (SFP+/SFP) 10 GigE/1 GigE или 6 портов (RJ45) 1 GigE (с внутренней функцией открытия при отказе)	4 порта (QSFP+) 40 GigE, 2 порта (QSFP+) 40 GigE, 8 портов (SFP+/SFP) 10 GigE/1 GigE или 6 портов (RJ45) 1 GigE (с внутренней функцией открытия при отказе)
10-гигабитный Ethernet	До 32	До 16	До 16
40-гигабитный Ethernet	До 16	До 10	До 10
Выделенные ответные порты (RJ45)	1 (10 Гбит/с / 1 Гбит/с / 100 Мбит/с)	1 (10 Гбит/с / 1 Гбит/с / 100 Мбит/с)	1 (10 Гбит/с / 1 Гбит/с / 100 Мбит/с)
Выделенные порты управления (RJ45)	1 (10 Гбит/с / 1 Гбит/с / 100 Мбит/с)	1 (10 Гбит/с / 1 Гбит/с / 100 Мбит/с)	1 (10 Гбит/с / 1 Гбит/с / 100 Мбит/с)
Выделенный порт для подключения устройства хранения данных (RJ45)	1 (10 Гбит/с / 1 Гбит/с / 100 Мбит/с)	1 (10 Гбит/с / 1 Гбит/с / 100 Мбит/с)	1 (10 Гбит/с / 1 Гбит/с / 100 Мбит/с)
Физические характеристики			
Габариты	2 x панель 2RU с креплением в стойку 43,79 см (Ш) x 17,48 см (В) x 73,05 см (Г)	Панель 2RU с креплением в стойку 43,79 см (Ш) x 8,74 см (В) x 73,05 см (Г)	Панель 2RU с креплением в стойку 43,79 см (Ш) x 8,74 см (В) x 73,05 см (Г)
Вес	60,8 кг	30,4 кг	30,4 кг
Хранение	600 ГБ (2 x твердотельный накопитель емкостью 300 ГБ в конфигурации RAID 1)	Твердотельный накопитель емкостью 300 ГБ в конфигурации RAID 1	Твердотельный накопитель емкостью 300 ГБ в конфигурации RAID 1
Максимальное энергопотребление	2 260 Вт	1 130 Вт	1 130 Вт
Резервный источник питания	Включено	Включено	Дополнительно
Электропитание	100 – 240 В (переменное напряжение; 50/60 Гц)		
Температура	0 °C – 35 °C (рабочая температура) -40 °C – 70 °C (температура хранения)		
Относительная влажность (без образования конденсата)	В рабочем состоянии: 10 % – 90 %; при хранении: 5 % – 95 %		
Высота над уровнем моря	0 – 3 000 м		
Сертификаты безопасности	Лицензия UL 1950, CSA-C22.2 № 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB и отчет, охватывающий все отклонения по странам.		
Сертификат EMI	FCC часть 15, класс A (CFR 47) (США), ICES-003 класс A (Канада), EN55022 класс A (Европа), CISPR22 класс A (международный)		

Спецификации McAfee Network Security Platform (продолжение)

Компоненты аппаратного обеспечения датчика	 NS7300	 NS7200	 NS7100
Производительность			
Реальная пропускная способность	5 Гбит/с	3 Гбит/с	1,5 Гбит/с
Максимальная пропускная способность (UDP, пакеты по 1 512 байт)	До 15 Гбит/с	До 10 Гбит/с	До 5 Гбит/с
Максимальное кол-во параллельных подключений	10 000 000	5 000 000	3 000 000
Кол-во соединений по TCP в секунду	225 000	200 000	135 000
Кол-во соединений по HTTP в секунду	135 000	128 000	115 000
Пропускная способность при использовании SSL (доля SSL-трафика: 10 %)	5 Гбит/с	3 Гбит/с	1,5 Гбит/с
Максимальное кол-во потоков SSL	500 000	400 000	250 000
Кол-во импортированных ключей SSL	1024	1024	1024
Типичная задержка	Менее 100 мкс	Менее 100 мкс	Менее 100 мкс
Кол-во виртуальных систем предотвращения вторжений (IPS)	1 000	1 000	1 000
Максимальное кол-во профилей DoS	5 000	5 000	5 000
Кол-во правил ACL	5 000	3 000	3 000
Порты			
Фиксированные порты Gigabit Ethernet, медные (внутренние, открыты при отказе)	8	8	8
Фиксированные порты 10 GigE/1 GigE (SFP +) (поддержка внешних пассивных устройств открытия при отказе)	2	2	2
Постоянные порты 40-Gigabit Ethernet	—	—	—
Гнезда для сетевых плат ввода-вывода	2	2	2
Сетевые платы ввода-вывода (5 вариантов)	4 разъема, 10 GigE/1 GigE, малой дальности, оптоволокно, 50 мкм, с функцией открытия при отказе; 4 разъема, 10 GigE/1 GigE, малой дальности, оптоволокно, 62,5 мкм, с функцией открытия при отказе; 4 разъема, 10 GigE/1 GigE, большой дальности, оптоволокно, с функцией открытия при отказе; 8 разъемов (SFP+/SFP), 10 GigE/1 GigE; или 6 разъемов (RJ45), 1 GigE с внутренней функцией открытия при отказе		
10-гигабитный Ethernet	До 18	До 18	До 18
40-гигабитный Ethernet	—	—	—
Выделенные ответные порты (RJ45)	1 (1 Гбит/с / 100 Мбит/с / 10 Мбит/с)	1 (1 Гбит/с / 100 Мбит/с / 10 Мбит/с)	1 (1 Гбит/с / 100 Мбит/с / 10 Мбит/с)
Выделенные порты управления (RJ45)	1 (1 Гбит/с / 100 Мбит/с / 10 Мбит/с)	1 (1 Гбит/с / 100 Мбит/с / 10 Мбит/с)	1 (1 Гбит/с / 100 Мбит/с / 10 Мбит/с)
Выделенный порт для подключения устройства хранения данных (RJ45)	1 (1 Гбит/с / 100 Мбит/с / 10 Мбит/с)	1 (1 Гбит/с / 100 Мбит/с / 10 Мбит/с)	1 (1 Гбит/с / 100 Мбит/с / 10 Мбит/с)
Физические характеристики			
Габариты	Панель 1RU с креплением в стойку 44,45 см (Ш) x 4,29 см (В) x 73,41 см (Г)	Панель 1RU с креплением в стойку 44,45 см (Ш) x 4,29 см (В) x 73,41 см (Г)	Панель 1RU с креплением в стойку 44,45 см (Ш) x 4,29 см (В) x 73,41 см (Г)
Вес	14 кг	14 кг	13 кг
Хранение	Твердотельный накопитель, 160 ГБ	Твердотельный накопитель, 160 ГБ	Твердотельный накопитель, 160 ГБ
Максимальное энергопотребление	350 Вт	350 Вт	250 Вт
Резервный источник питания	Дополнительно	Дополнительно	Дополнительно
Электропитание	100 – 240 В (переменное напряжение; 50/60 Гц)		
Температура	0 °C – 35 °C (рабочая температура) -40 °C – 70 °C (температура хранения)		
Относительная влажность (без образования конденсата)	В рабочем состоянии: 10 % – 90 %; при хранении: 5% – 95%		
Высота над уровнем моря	0 – 3 000 м		
Сертификаты безопасности	Лицензия UL 1950, CSA-C22.2 № 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB и отчет, охватывающий все отклонения по странам.		
Сертификат EMI	FCC часть 15, класс A (CFR 47) (США), ICES-003 класс A (Канада), EN55022 класс A (Европа), CISPR22 класс A (международный)		

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