McAfee Network Threat Behavior Analysis

Сбор полной информации о действиях и угрозах в сети

Решение McAfee® Network Threat Behavior Analysis, входящее в линейку продуктов McAfee, — интегрированный компонент платформы McAfee Network Security Platform, позволяющий в режиме реального времени собирать информацию о состоянии сетевой инфраструктуры и защищать ее от угроз безопасности. Анализируя трафик, идущий от коммутаторов и маршрутизаторов, McAfee Network Threat Behavior Analysis обнаруживает в сети опасные действия и эффективно предотвращает скрытые атаки. Оно проводит комплексную оценку угроз сетевого уровня, собирает информацию об общем характере поведения каждого элемента сети и дает возможность мгновенно выделять основные признаки потенциальных видов аномалий и атак, таких как вредоносные программы, атаки «нулевого дня», бот-сети и черви. McAfee Network Threat Behavior Analysis включает в себя также некоторые передовые модули, входящие в состав платформы McAfee Network Security Platform, в частности модуль эмуляции, работающий в режиме реального времени и позволяющий выявлять вредоносные программы без использования сигнатур.

Автоматизированный сбор информации о скрытых атаках

Являясь объектом сложных скрытых атак, не поддающихся обнаружению с помощью традиционных методов обнаружения, ваша сеть подвержена риску серьезных нарушений безопасности и сбоев в работе. Анализируя трафик, идущий от коммутаторов и маршрутизаторов, McAfee Network Threat Behavior Analysis в автоматическом режиме отслеживает необычное поведение и сообщает о нем. Это дает вам возможность выявлять атаки на вашу сеть и быстро на них реагировать.

Используя данные NetFlow и J-Flow, аппаратное устройство McAfee Network Threat Behavior Analysis выявляет угрозы за пределами обычного периметра систем предотвращения вторжений (IPS). Оно оснащено всем необходимым: четырехъядерными процессорами, дисковым массивом RAID и сетевым подключением по стандарту Gigabit Ethernet. Кроме того, оно может подключаться к автономным сетям хранения данных (SAN). Благодаря хорошей пропускной способности оно может обрабатывать большие объемы сетевого трафика, что позволяет быстрее анализировать трафик.

Ключевые преимущества

Сбор информации для защиты сети

- Мониторинг и учет необычного сетевого поведения путем анализа сетевого трафика
- Упреждающее обнаружение угроз на основе анализа поведения
- Эффективное обнаружение неизвестных угроз
- Обнаружение аномалий включает в себя обнаружение атак «нулевого дня», нежелательных сообщений, бот-сетей и попыток зондирования сети

Комплексная защита от вредоносных программ

- Блокирование вредоносных программ путем эмуляции поведения вредоносных файлов в режиме реального времени
- Расширенное сопоставление (корреляция) данных в масштабах всей вашей сети с целью обнаружения бот-сетей
- Сбор на конечных точках и сопоставление (корреляция) данных о сетевых потоках и событиях

Непревзойденные функции сбора и анализа информации о сети

При принятии решений, касающихся приложений и протоколов в вашей сети, вы сможете руководствоваться конкретной информацией, полученной с помощью решения McAfee Network Threat Behavior Analysis. Оно отслеживает необычное сетевое поведение и сообщает о нем, чтобы затем выявлять угрозы, используя бихевиористические алгоритмы. Выявление аномалий путем анализа поведения узлов и приложений включает в себя обнаружение атак «нулевого дня», нежелательных сообщений, бот-сетей и попыток зондирования сети. Комплексный анализ потока данных позволяет быстро выявлять случаи использования несанкционированных приложений и определять проблемные сегменты сети.

Контроль и предотвращение эпидемий вредоносных программ

Благодаря взаимодействию с McAfee Network Security Platform решение McAfee Network Threat Behavior Analysis дает возможность с помощью эмуляции поведения в режиме реального времени проверять и блокировать подозрительные файлы. Модуль эмуляции в режиме реального времени выполняет проверку подозрительных файлов с целью обнаружения и блокирования вредоносного поведения. Используя расширенные функции сопоставления (корреляции) данных, получаемых с большого количества систем IPS и сетевых устройств, McAfee Network Threat Behavior Analysis обнаруживает скрытые бот-сети, способные обходить традиционные средства защиты, работающие на основе сигнатур. Взаимодействие с агентом McAfee Endpoint Intelligence Agent позволяет обнаруживать и блокировать взломанные конечные точки, передающие вредоносный трафик под видом допустимого. Анализ активности конечных точек на основе репутации отграничивает утечку данных и предотвращает эпидемии вредоносных программ.

Возможность упорядочить операции по обеспечению безопасности и сэкономить средства

Устройство McAfee Network Threat Behavior Analysis обеспечивает сбор всех оперативных данных, необходимых для экономически эффективного управления безопасностью. Оно сокращает время реагирования на инциденты, повышает быстродействие сетей и обеспечивает непрерывность бизнес-процессов, блокируя сетевые угрозы и средства использования уязвимостей.

Дополнительные функции

- Повышение уровня защиты благодаря интеграции с McAfee Global Threat Intelligence (McAfee GTI)
- Виртуальный вариант для экономичных решений
- Расширение функций сбора и сопоставления данных благодаря интеграции с McAfee ePolicy Orchestrator® (McAfee ePO™), McAfee Enterprise Security Manager и McAfee Vulnerability Manager
- Упрощение процесса сортировки и анализа сетевого трафика
- Панель мониторинга метаданных по потокам (идентификаторы приложений, файлы, URL-адреса)
- Повышение общего уровня безопасности благодаря комплексным функциям карантина
- Сбор информации о внешних узлах и подробная оценка узлов по факторам угроз
- Совместимость с коммутаторами и маршрутизаторами Cisco (NetFlow v5 и v9) и Juniper (J-Flow v5 и v9)

ЛИСТ ДАННЫХ

	NTBA T-600	NTBA T-1200
Спецификации		
Кол-во потоков в секунду	до 60 000	до 100 000
Cisco NetFlow	v5 и v9	v5 и v9
Juniper J-Flow	v5 и v9	v5 и v9
Процессор	1 процессор Xeon E5-2658	2 процессора Xeon E5-2658
Память	46 ГБ	96 ГБ
Полезный объем хранилища	4,4 ТБ/Raid 10	8,8 ТБ/Raid 10
Сетевые интерфейсы	4 медных порта (10/100/1000)	4 медных порта (10/100/1000)
Условия эксплуатации		
Форм-фактор	1U	2U
Ширина	43,8 см	43,8 см
Глубина	70,94 см	70,78 см
Высота	4,32 см	8,76 см
Макс. вес	14,96 кг	21,6 кг
Примерная потребляемая мощность (худший сценарий)	402 Вт	667 Вт
Резервный источник питания	750 Вт	750 Вт
Требования к охлаждению системы	1 370 БТЕ/час	2 280 БТЕ/час
Температура при эксплуатации	+10...+35 °C; скорость изменения температуры не должна превышать 10 °C в час	

Спецификации виртуального варианта NTBA	T-VM	T-100VM	T-200VM
Рекомендуемый объем ОЗУ	16 ГБ	8 ГБ	16 ГБ
Рекомендуемое кол-во ЦП	4	4	4
Кол-во потоков в секунду	до 25 000	до 10 000	до 25 000

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