McAfee Advanced Threat Defense

Обнаружение сложных направленных атак

Основные отличительные качества McAfee Advanced Threat Defense

Тесная взаимосвязь решений Intel Security

- Сокращение разрыва между обнаружением атаки и ее сдерживанием и обеспечением защиты в масштабе всей организации
- Оптимизация рабочих процессов, позволяющая быстрее реагировать на угрозы и быстрее их устранять

Эффективные функции обнаружения угроз

- Мощные средства распаковки программ, обеспечивающие более эффективный и полный анализ содержимого
- Сочетание передовых методов статического анализа кода и динамического анализа файлов, позволяющее более точно обнаруживать угрозы, используя уникальные аналитические данные

Централизованный анализ вредоносных программ

- Использование модуля анализа вредоносного ПО в режиме совместного доступа, позволяющее сократить количество необходимых устройств в сети и снизить расходы
- Упрощенное развертывание

Продукт McAfee® Advanced Threat Defense, входящий в линейку продуктов Intel Security®, дает организациям возможность выявлять целенаправленные атаки повышенной сложности и немедленно преобразовывать информацию об угрозах в меры реагирования и обеспечения безопасности. В отличие от традиционных изолированных сред («песочниц») в него включены дополнительные средства проверки, расширяющие возможности обнаружения угроз и выявления методов обхода защиты. Тесная взаимосвязь решений Intel Security для защиты сетей, конечных точек и т. д. обеспечивает мгновенный обмен информацией об угрозах в масштабах всей среды. Это позволяет укрепить защиту и оптимизировать процессы расследования инцидентов.

Наша технология преобразила процесс обнаружения угроз, объединив функции анализа сложного вредоносного ПО с существующими средствами защиты, расположенными в разных точках сети (от периферии до конечных точек), и обеспечив обмен информацией об угрозах в рамках всей ИТ-среды. Обмен информацией об угрозах между управляющими системами и системами защиты сетей и конечных точек позволяет нашим решениям моментально блокировать доступ удаленного центра управления к взломанным системам, помещать их в карантин, блокировать другие экземпляры таких же или похожих угроз, оценивать размер возможного ущерба и принимать меры.

McAfee Advanced Threat Defense: обнаружение угроз повышенной сложности

Благодаря использованию новаторского многоуровневого подхода решение McAfee Advanced Threat Defense способно обнаруживать современные скрытые вредоносные программы «нулевого дня». Система включает средства анализа сигнатур с незначительным влиянием на производительность, репутации и эмуляции в режиме реального времени с детальным статическим и динамическим анализом в «песочнице» с целью оценки реального поведения программ. Все эти средства в комплексе представляют собой самую надежную из представленных на рынке систему защиты от вредоносных программ, обеспечивая разумное равновесие между требованиями безопасности и быстродействия.

intel Security

Интегрированные решения

- **McAfee Email Gateway**
- **McAfee Enterprise Security Manager**
- **McAfee ePolicy Orchestrator**
- **McAfee Network Security Platform**
- **McAfee Next Generation Firewall**
- **McAfee Threat Intelligence Exchange**
- **McAfee Web Gateway**

Использование методов, отличающихся невысокой интенсивностью анализа, таких как сигнатуры и эмуляция в режиме реального времени, позволяет обнаруживать известные вредоносные программы и положительно сказывается на быстродействии. Использование же полного статического анализа кода в дополнение к технологии «песочницы» позволяет обеспечить защиту от более широкого спектра чрезвычайно замаскированных, трудноуловимых угроз и на основе подробной классификационной информации о вредоносном ПО выявлять родственное вредоносное ПО, в котором используются уже известные фрагменты кода. Распаковка и полный статический анализ кода позволяет обнаруживать такие методы обхода «песочницы», как пути для отложенного и условного выполнения, которые в динамической среде нередко не запускаются.

Упаковка кода дает разработчикам вредоносных программ возможность изменять состав кода или скрывать его с целью избежания обнаружения. Большинство продуктов не может правильно распаковывать весь исходный исполняемый код, подлежащий анализу. В McAfee Advanced Threat Defense включены мощные функции распаковки, позволяющие «распутать» код и добраться до исходного исполняемого кода. Это дает возможность с помощью статического анализа кода искать аномалии за пределами высокоуровневых файловых атрибутов, анализируя все атрибуты и наборы инструкций с целью выявления его намерений.

Статический анализ кода и динамический анализ файлов, используемые в совокупности, позволяют провести полную и подробную оценку ПО, подозреваемого во вредоносности.

Анализ угрозы в «песочнице», учитывающей особенности целевой среды, повышает точность обнаружения

Администраторы имеют возможность загружать и анализировать объекты, используя набор индивидуально настроенных виртуальных машин или «золотых» образов. Это позволяет организациям выполнять анализ угроз с точным воссозданием профиля целевой системы вместо универсального образа, что существенно повышает точность оценки рисков.

При том, что в сети организации может одновременно использоваться множество профилей систем («золотых образов»), решение McAfee Advanced Threat Defense направляет в программное обеспечение McAfee ePolicy Orchestrator® (McAfee ePO™) запросы на определение операционных систем хостов и составление перечня приложений, чтобы анализ файлов выполнялся с учетом условий конкретных целевых систем.

Усиление защиты

Обнаружение сложных вредоносных программ крайне важно. Но если всё, на что способно решение, это генерирование отчета и отсылка уведомления, то администраторам все равно нужно выполнять огромный объем работы, а сеть остается незащищенной.

Благодаря тесной интеграции между McAfee Advanced Threat Defense и защитными устройствами, расположенными в разных точках сети (от периферии до конечных точек), интегрированные защитные устройства могут принимать меры реагирования сразу, как только McAfee Advanced Threat Defense классифицирует тот или иной файл как вредоносный. Такая тесная автоматическая интеграция средств обнаружения и защиты имеет ключевое значение.

McAfee Advanced Threat Defense допускает два способа интеграции: прямая интеграция с отдельными защитными решениями и опосредованная интеграция через McAfee Threat Intelligence Exchange.

Прямая интеграция дает защитным решениям Intel Security возможность немедленно принимать необходимые меры в отношении файлов, проанализированных с помощью McAfee Advanced Threat Defense. Возможность немедленно встроить информацию об угрозах в существующие процессы применения политик позволяет не допускать в сеть другие экземпляры таких же или похожих файлов.

Результаты анализа, проведенного McAfee Advanced Threat Defense, отображаются в журналах интегрированных продуктов и на их панелях мониторинга, как если бы весь анализ был выполнен самими этими продуктами. Это оптимизирует рабочие процессы и дает администраторам возможность эффективно управлять оповещениями, работая через один-единственный интерфейс.

Интеграция с McAfee Threat Intelligence Exchange дает дополнительным защитным продуктам (включая McAfee Endpoint Protection) возможность использовать функции McAfee Advanced Threat Defense. Таким образом, широкий спектр интегрированных защитных решений получает доступ к результатам анализа и признакам взлома. Когда McAfee Advanced Threat Defense признает файл вредоносным, McAfee Threat Intelligence Exchange передает информацию об угрозах всем имеющимся в организации интегрированным средствам защиты путем обновления данных о репутации.

Конечные точки, подключенные к McAfee Threat Intelligence Exchange, получают возможность заблокировать первоначальную установку вредоносных программ и обеспечить упреждающую защиту на случай, если они столкнутся с этим файлом в будущем. А шлюзы, подключенные к McAfee Threat Intelligence Exchange, не допустят этот файл внутрь организации.

Кроме того, подключенные к McAfee Threat Intelligence Exchange конечные точки получают результаты анализа файлов даже будучи отключенными от сети. Это позволяет избавиться от белых пятен, возникающих в результате внеполосной доставки полезной нагрузки.

Обнаружение и исправление взломанных систем

Чтобы устранить последствия атаки, организациям необходимы решения, позволяющие комплексно собирать информацию о происходящем и приоритизировать информацию об угрозах. Это даст возможность принимать более обоснованные решения и адекватно реагировать на угрозы. Взаимодействуя между собой, McAfee Enterprise Security Manager, McAfee Endpoint Protection и McAfee Threat Intelligence Exchange дают организациям именно то, что нужно.

Сопоставляя получаемые из McAfee Advanced Threat Defense и других систем безопасности подробные данные о репутации файлов и событиях выполнения файлов, McAfee Enterprise Security Manager генерирует расширенное представление данных за текущий и прошлые периоды, дающее администраторам возможность лучше ориентироваться в угрозах безопасности, приоритизировать риски и контролировать ситуацию в режиме реального времени. Отслеживая базовые уровни событий на конечных точках, решение динамически реагирует на значительные отклонения и установленные пороговые значения, корректируя уровень рисков для пользователей и активов. McAfee Enterprise Security Manager дает четкое представление о риске, что позволяет немедленно принимать меры по исправлению ситуации в интерактивном или автоматизированном режимах. Тесная интеграция с McAfee Endpoint Protection и McAfee Threat Intelligence Exchange позволяет осуществлять такие действия по упреждающему смягчению риска, как создание новых конфигураций, внедрение новых политик, удаление файлов и развертывание обновлений программного обеспечения.

Развертывание
McAfee Advanced Threat Defense представляет собой централизованно развертываемое аппаратное устройство для анализа сложных вредоносных программ, легко интегрируемое с уже приобретенными вами защитными решениями McAfee. McAfee Advanced Threat Defense функционирует как общий ресурс для различных защитных устройств Intel Security, экономически эффективно масштабируемый в пределах всей сети. Центры управления операциями по обеспечению безопасности и аналитики вредоносных программ могут также использовать McAfee Advanced Threat Defense для расследования инцидентов: для этого предусмотрена возможность ручного ввода данных. Наличие широкого набора функций распаковки позволяет сократить время расследования инцидентов с нескольких дней до нескольких минут. Если сводные отчеты McAfee Advanced Threat Defense помогают получить общее представление о приоритизации угроз и принимаемых мер, то дополнительные подробные отчеты (от результатов дизассемблирования файлов до графических диаграмм вызовов функций и информации о встроенных или перемещенных файлах) служат источником информации, крайне необходимой аналитикам для расследования инцидентов.

За дополнительной информацией о McAfee Advanced Threat Defense или для получения ознакомительной версии решения просим обращаться к представителю или на страницу **www.mcafee.com/ru/products/advanced-threat-defense.aspx**.

Технические характеристики McAfee Advanced Threat Defense	**ATD-3000**	**ATD-6000**
Форм-фактор	1RU с креплением на стойке	2RU с креплением на стойке
Производительность	До 150 000 объектов в сутки	До 250 000 объектов в сутки
Обнаружение	**ATD-3000/ATD-6000**	
Поддерживаемые типы файлов/носителей	PE-файлы, файлы Adobe, Microsoft Office, архивные файлы, файлы Java, Android Application Package	
Методы анализа	McAfee Anti-Malware Engine, оценка репутации файлов с помощью технологии McAfee GTI, Gateway Anti-Malware (эмуляция и анализ поведения), динамический анализ (в «песочнице»), статический анализ кода	
Поддерживаемые операционные системы	Windows 8 (32- и 64-разрядные версии), Windows 7 (32- и 64-разрядные версии), Windows XP (32- и 64-разрядные версии), Windows Server 2003, Windows Server 2008 (64-разрядная версия); Android	

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