McAfee Advanced Threat Defense

Обнаружение сложных целенаправленных атак

Ключевые преимущества 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 методов детального анализа кода и динамического анализа файлов, позволяющее более точно обнаруживать угрозы, используя уникальные аналитические данные

Гибкое централизованное развертывание

- Сокращение затрат благодаря централизованному развертыванию с поддержкой множества протоколов
- Несколько вариантов развертывания позволяют интегрировать данный продукт в любую сеть

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. Несколько вариантов развертывания позволяют интегрировать данный продукт в любую сеть.

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 проверки сигнатур с незначительным влиянием на производительность, репутации и эмуляции в режиме реального времени с детальным 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 Active Response
- McAfee Enterprise Security Manager
- McAfee ePolicy Orchestrator
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
  - McAfee Application Control
  - McAfee Endpoint Protection
  - McAfee Server Security
- 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 детального анализа кода в дополнение к технологии «песочницы» позволяет обеспечить защиту от более широкого спектра хорошо замаскированных и трудноуловимых угроз. Оно позволяет получать подробную классификационную информацию о вредоносном ПО, включая анализ схожести кода с известными семействами вредоносного ПО, отличающихся использованием одного и того же кода в разных программах. Распаковка и детальный 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 детального статического анализа кода искать аномалии за пределами высокоуровневых файловых атрибутов, анализируя все атрибуты и наборы инструкций с целью выявления его намерений.

Детальный статический анализ кода и динамический анализ файлов, используемые в совокупности, позволяют провести полную и подробную оценку ПО, подозреваемого во вредоносности. Уникальные результаты анализа формируют сводные отчеты, которые дают полное представление о текущей ситуации и позволяют приоритизировать действия, а кроме того, обеспечивают предназначенные для аналитиков данных более подробные отчеты, содержащие данные о вредоносных программах.

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

Для устранения последствий атак организациям необходимо иметь комплексное представление о происходящем, подкрепленное приоритизированной информацией об угрозах и позволяющее принимать более обоснованные решения и адекватно реагировать на угрозы. Именно этого позволяет добиться использование взаимодействующих между собой решений McAfee.

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.

Информация о признаках взлома, получаемая из McAfee Advanced Threat Defense, дает McAfee Enterprise Security Manager возможность искать признаки наличия таких артефактов во всех сохраненных им данных о сети и системах за период до шести месяцев. Это позволяет выявлять системы, ранее обменивавшиеся данными с только что выявленными источниками вредоносного ПО. 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, McAfee Threat Intelligence Exchange и McAfee Active Response позволяет оптимизировать скорость реагирования на инциденты и эффективность мер по обеспечению безопасности благодаря наличию информации о происходящем и возможности выполнять такие действия по упреждающему снижению риска, как создание новых конфигураций, внедрение новых политик, удаление файлов и развертывание обновлений программного обеспечения. Автоматическое выявление зараженных конечных точек по всей сети организации с помощью McAfee Active Response и включение их в отчеты McAfee Advanced Threat Defense позволяет быстро принимать меры на основе фактической информации.

Развертывание

Несколько вариантов развертывания системы анализа угроз повышенной сложности позволяют интегрировать данный продукт в любую сеть. Решение Advanced Threat Defense предлагается для развертывания как в виде аппаратного устройства, так и в виртуальной форме. Все варианты развертывания работают в качестве совместного ресурса для нескольких решений Intel Security, обеспечивая экономически эффективное масштабирование и снижение издержек.

Центры управления операциями по обеспечению безопасности и аналитики вредоносных программ могут также использовать McAfee Advanced Threat Defense для расследования инцидентов.

McAfee Advanced Threat Defense включает в себя целый ряд дополнительных функций:

- Поддержка опции настраиваемого образа: оценка угроз осуществляется с учетом индивидуального профиля узла.
- Интерактивный пользовательский режим: дает аналитикам возможность напрямую взаимодействовать с образцами вредоносных программ.
- Широкий набор функций распаковки: позволяет сократить время расследования инцидентов с нескольких дней до нескольких минут.
- Полный логический путь: позволяет проводить более глубокий анализ образцов, вынуждая код выполнять дополнительные логические пути, не выполняемые в стандартных изолированных средах.
- Отправка образца в несколько разных виртуальных сред: повышает скорость проведения расследований, поскольку позволяет определить, какие переменные среды необходимы для выполнения анализируемого файла.
- Подробные отчеты о результатах дизассемблирования, отображение содержания оперативной памяти в виде диаграммы вызова графической функции, внедренные или перемещенные файлы, журналы API пользователя и информация в формате PCAP: 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 своему представителю или на страницу **www.mcafee.com/ru/products/advanced-threat-defense.aspx**.

Технические характеристики McAfee Advanced Threat Defense		
Вариант аппаратного устройства	ATD-3000 Корпус 1RU для монтажа в стойку	ATD-6000 Корпус 2RU для монтажа в стойку
Вариант виртуального устройства	v1008, v1016, v3032, v6064 ESXi 6.0	v1008, v1016, v3032, v6064 ESXi 6.0
Обнаружение		
Поддерживаемые типы образцов файлов	PE-файлы, файлы Adobe, Microsoft Office, файлы изображений, архивные файлы, файлы Java, Android Application Package, URL-адреса	
Методы анализа	McAfee Anti-Malware Engine, оценка репутации файлов, URL-адресов и IP-адресов с помощью технологии GTI, Gateway Anti-Malware (эмуляция и анализ поведения), динамический анализ (в «песочнице»), детальный анализ кода, пользовательские правила для YARA	
Поддерживаемые операционные системы	Windows 10 (64-разрядная версия), Windows 8.1 (64-разрядная версия), Windows 8 (32- и 64-разрядные версии), Windows 7 (32- и 64-разрядные версии), Windows XP (32- и 64-разрядные версии), Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003; Android Поддержка операционной системы Windows на всех языках	
Форматы вывода данных	STIX, OpenIOC, XML, JSON, HTML, PDF, текст	
Методы предоставления	Интегрированные продукты, прямые/ручные, API	

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

Октябрь 2016 г.