Malwarebytes Incident Response

Централизованное обнаружение и нейтрализация вредоносных объектов

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Ядро Incident Response
Быстрая и чрезвычайно эффективная проверка на наличие вирусов, которая может запускаться по требованию, согласно расписанию или автоматически

Несколько режимов проверки
Специальные типы проверки – быстрая, полная и выборочная – позволяют не прерывать работу конечного пользователя во время поиска угроз

Linking Engine
Бессигнатурная технология, которая обнаруживает и полностью удаляет артефакты вирусов, связанные с основной вредоносной нагрузкой

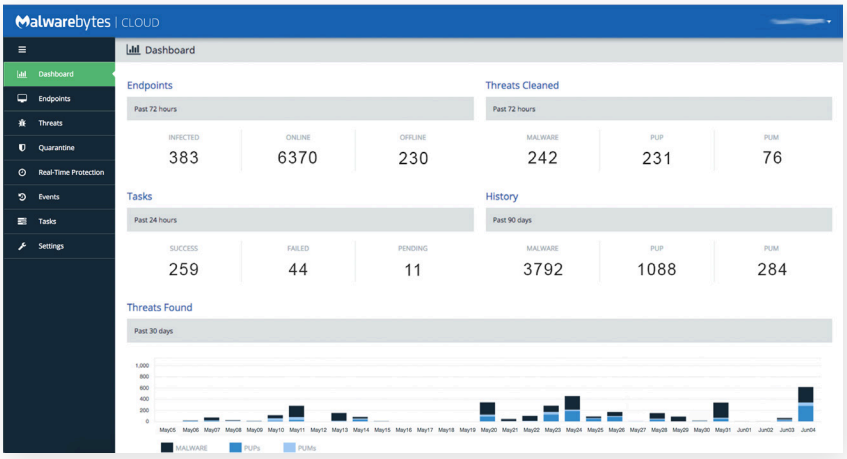
Облачная платформа Malwarebytes
Панель управления, работающая на основе облачных технологий, предоставляет все средства для простого централизованного управления политикой безопасности, установкой программ и составлением отчетов

Агент Asset Management
В удобной форме предоставляет подробные сведения о компьютерах в сети, в том числе об объектах в памяти, установленных программах, программах автозагрузки и других параметрах

Forensic Timeliner
Собирает информацию о событиях журналов Windows и отображает полученные сведения в хронологическом порядке

Современные вредоносные программы используют все более изощренные алгоритмы атаки на своих жертв с целью получения их личных данных. Вирусы продолжают проникать на компьютеры предприятий, школ и государственных учреждений даже в том случае, если они инвестировали миллионы в укрепление средств защиты своих сетей. На устранение последствий этих атак[1] требуется много времени и усилий – может понадобиться 6–8 часов, чтобы полностью удалить вирус или переустановить из образа систему каждого зараженного компьютера. По результатам исследования, проведенного институтом Ponemon, вредоносные объекты, проникшие на компьютеры предприятия, остаются незамеченными в среднем на протяжении 229 дней, после чего обычно требуется еще 82 дня[2], чтобы удалить из системы их следы. Поэтому бизнесу нужно вооружить своих специалистов по безопасности самыми современными средствами телеметрии, а также лучшими программами, способными нейтрализовать угрозы.

Именно таким инструментом и является программа Malwarebytes Incident Response. Это превосходное средство обнаружения и нейтрализации вредоносных объектов, которое использует масштабируемую платформу управления, работающую на основе облачных технологий. Данная программа проверяет компьютеры в сети, выявляя и полностью удаляя даже самые совершенные угрозы, в том числе вредоносное ПО, потенциально нежелательные программы и рекламное ПО. Malwarebytes Incident Response не только эффективно обнаруживает вирусы, но и существенно сокращает время нейтрализации их атак благодаря широкой масштабируемости и автоматизации, а также непревзойденной приспосабливаемости к постоянно меняющимся условиям.



Информационная панель облачной платформы Malwarebytes

Примечания

[1] *Устранение последствий атак (Incident response) означает применение инструментов, процессов и кадровых ресурсов той или иной организации с целью нейтрализовать кибератаку после ее обнаружения, а также устранить причиненный ею ущерб.*

[2] *Источник: Ponemon Institute, 2016 Cost of Data Breach Study (Исследование последствий утечки данных 2016), июнь 2016 г.*

Ключевые преимущества

Автоматизация

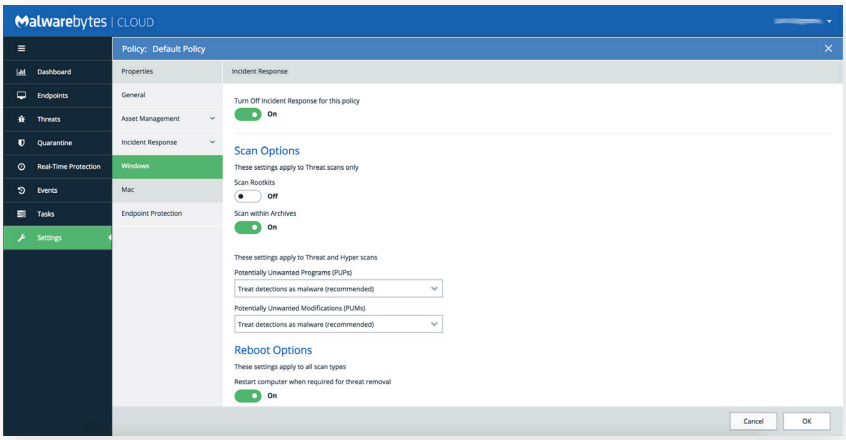
Установив программу Malwarebytes Incident Response на компьютеры в сети своего предприятия, Вы получите надежное средство обнаружения и нейтрализации вредоносных объектов, всегда готовое к использованию по нажатию кнопки. Эта программа прекрасно интегрируется в существующую инфраструктуру SIEM и систему управления компьютерами в сети, а также отлично взаимодействует с другими защитными инструментами, что позволяет ей автоматически реагировать на любые попытки вредоносных программ проникнуть на Ваши компьютеры. Автоматизированное реагирование на угрозы позволяет предприятиям оптимизировать ресурсы, затрачиваемые на преодоление чрезвычайных ситуаций, а также сокращает время обнаружения вредоносных объектов на компьютерах.

Гибкость

Программа Malwarebytes Incident Response использует единый постоянный агент, а также включает дополнительные непостоянные агенты (Breach Remediation). Это обеспечивает гибкость данного решения и расширяет возможности для его установки в динамично развивающейся информационной среде предприятий. Продукт Malwarebytes легко интегрируется с существующими средствами защиты, а также отвечает всем требованиям Вашей инфраструктуры и операционной системы (Windows и Mac OS X).

Масштабируемость

Программа Malwarebytes Incident Response предоставляется посредством новой облачной платформы Malwarebytes, предназначенной для управления компьютерами в сети. Благодаря облачной платформе Malwarebytes данное решение является простым в использовании: Вы без проблем можете установить и применять программу Malwarebytes Incident Response или другие продукты Malwarebytes независимо от того, сколько компьютеров Вам нужно защитить – один или миллион. Централизованная облачная платформа также избавит Вас от затрат на приобретение и обслуживание локального аппаратного обеспечения.



Malwarebytes Incident Response: настройка политики безопасности

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Компоненты

- Облачная платформа Malwarebytes
- Malwarebytes Incident Response (постоянные агенты для Windows и Mac OS X)
- Breach Remediation (непостоянные агенты для Windows (CLI) и Mac (GUI и CLI))
- Forensic Timeliner (Windows)
- Поддержка по электронной почте и телефону

Требования к аппаратному обеспечению

Windows

Процессор: 1 ГГц
ОЗУ: 1 ГБ (клиенты); 2 ГБ (серверы)
Место на диске: 100 МБ (программа + журналы)
Активное подключение к сети Интернет

Mac

Любое устройство Apple Mac, поддерживающее Mac OS X (10.10 или более поздней версии)
Активное подключение к сети Интернет

Поддерживаемые операционные системы

Windows 10® (32-bit, 64-bit)
Windows 8.1® (32-bit, 64-bit)
Windows 8® (32-bit, 64-bit)
Windows 7® (32-bit, 64-bit)
Windows Vista® (32-bit, 64-bit)
Windows XP® SP3 (только 32-bit)
* Windows Server 2016® (32-bit, 64-bit)
* Windows Server 2012/2012R2® (32-bit, 64-bit)
* Windows Small Business Server 2011
* Windows Server 2008/2008R2® (32-bit, 64-bit)
* Windows Server 2003® (только 32-bit)

Mac OS X (10.10 или более поздней версии)

Пожалуйста, обратите внимание, что системы Windows Server, которые используют вариант установки Server Core, исключены из данного списка.

* *В операционных системах Windows Server не поддерживается интеграция с Центром поддержки Windows.*

malwarebytes.com
corporate-sales@malwarebytes.com
1.800.520.2796

Компания Malwarebytes предлагает новые технологии киберзащиты, которым доверяют миллионы пользователей во всем мире. Malwarebytes проактивно защищает частных пользователей и целые компании от опасных угроз, в числе которых вредоносное ПО, программы-вымогатели и эксплойты, постоянно ускользающие от обычных антивирусных средств. Флагманский продукт компании сочетает в себе совершенные средства эвристического анализа и бессигнатурные технологии выявления угроз, что позволяет блокировать кибератаку до того, как системе будет нанесен ущерб. Продуктами Malwarebytes пользуются более 10 000 компаний по всему миру – они доверяют нашим программам и рекомендуют их всем пользователям. Компания Malwarebytes была основана в 2008 году, ее главный офис расположен в Калифорнии. На сегодняшний день компания располагает не только рядом представительств в Европе и Азии, но и международной командой профессионалов, в которую входят исследователи киберугроз и специалисты в области компьютерной безопасности.