TeamViewer | Malwarebytes

КРАТКОЕ ОПИСАНИЕ РЕШЕНИЯ

Расширенная киберзащита от вредоносных программ и угроз нулевого дня

Malwarebytes обнаруживает, идентифицирует, блокирует и изолирует вредоносное ПО, защищая конечные устройства как от известных угроз, так и от атак повышенной сложности.

Почему организациям нужна улучшенная защита конечных устройств

Конечные устройства — легкая мишень для киберпреступников. В отличие от серверов, их безопасности не уделяется столько внимания, поэтому они более уязвимы для кибератак. С ростом числа удаленных сотрудников и распространением политик работы на личных устройствах (BYOD) в сетях компаний используется все больше конечных устройств. А чем меньше их контроль со стороны ИТ-отдела, тем привлекательнее они для злоумышленников.

Киберпреступники научились запускать атаки повышенной сложности, которые обнаруживают уязвимости в конечных устройствах, распространяются по сети и причиняют ущерб, устранение которого дорого обходится компании.

Почему многие решения для защиты конечных устройств не способны эффективно обнаруживать угрозы повышенной сложности

Традиционные решения для защиты конечных устройств ищут на компьютерах только сигнатуры известных вредоносных программ и сканируют систему на алгоритмы атаки методом подбора паролей.

Но самую большую угрозу для конечных устройств сегодня представляют новые и неизвестные атаки (атаки повышенной сложности), когда нет ни сигнатур, ни известного алгоритма, который могло бы обнаружить сканирование. Такая атака повышенной сложности может быть настолько новой, что поставщики антивирусных программ еще не знают о ней. Либо угроза могут месяцами или годами незаметно скрываться в системе, а затем внезапно атаковать в момент обнаружения уязвимости: в «нулевой день».

Традиционные антивирусные решения не распознают атаки новых видов. Единственные атаки повышенной сложности, которые уверенно обнаруживаются — это те, что использовались и регистрировались ранее. Не умея достоверно находить новые атаки, такие антивирусы дают высокий процент ложных срабатываний, отправляя ИТ-отделы на поиски несуществующих угроз.

Между тем, количество известных угроз растет с каждым днем, их базы данных постоянно расширяются, и конца этому не видно. Из-за большого объема баз данных известного вредоносного ПО антивирус отвлекает значительные системные ресурсы и замедляет работу защищаемых устройств.

Malwarebytes использует другой подход.

Ключевые преимущества

Оперативная аналитика

Быстрое получение аналитических данных с помощью автоматического анализа угроз и оценки потенциальных воздействий позволяет руководителям подразделений информационной безопасности своевременно предупреждать руководство о потенциальных рисках, смягчая проблемы и предотвращая эскалацию инцидентов.

Высокая производительность

Всего один легкий агент позволяет быстро выявить и заблокировать запуск вредоносного кода, не замедляя устройство.

Простая архитектура без сценариев

Благодаря комплексным функциям безопасности конечных устройств и автоматизированным возможностям справиться с вредоносным ПО можно без сложных процедур — достаточно пары щелчков мышью.

Как работает Malwarebytes

В отличие от традиционных решений для защиты конечных устройств, Malwarebytes имеет небольшой размер и не влияет их работу. Как?

Вместо того, чтобы собирать данные о вредоносных программах, Malwarebytes распознает и вносит в каталог «хорошее» ПО — правильно подписанный код от известных поставщиков. Проанализировав код и установив, что он соответствует известному «хорошему» ПО, Malwarebytes позволяет ему продолжить выполнение любого процесса.

Если же код не удается соотнести с известным «хорошим» ПО, Malwarebytes изолирует его, пока не определит, хороший он или вредоносный. Со временем машинное обучение позволяет Malwarebytes все быстрее и точнее выносить упреждающие вердикты для вредоносных программ.

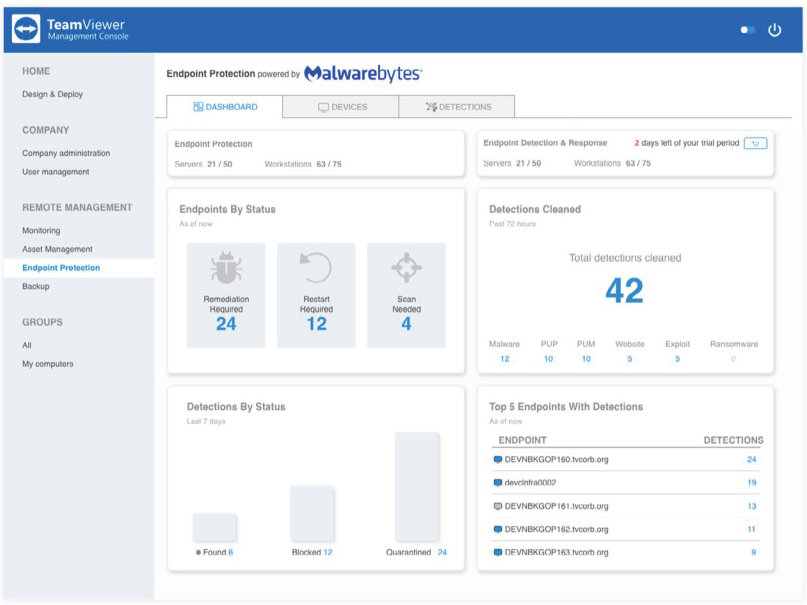

Рисунок 1. Панель управления Malwarebytes в консоли TeamViewer Management Console представляет интерактивный обзор всей активности вредоносного ПО в вашей ИТ-инфраструктуре, способов его обработки и требующих внимания устройств.

Malwarebytes Endpoint Protection (EPP) и Malwarebytes Endpoint Detection and Response (EDR)

Оба решения — Malwarebytes Endpoint Protection и Malwarebytes Endpoint Detection and Response — можно массово развернуть в автоматическом режиме с помощью TeamViewer, не мешая работе пользователей.

Malwarebytes Endpoint Protection

Malwarebytes Endpoint Protection обеспечивает облачную защиту от вредоносного ПО и его устранение благодаря точному обнаружению, упреждающему блокированию и тщательному устранению угроз. Решение EPP полностью масштабируется и удобно для организаций любого размера.

Благодаря облегченному агенту Malwarebytes EPP обеспечивает полноценную работу конечных устройств, так что вам не придется выбирать между защитой и производительностью. А поскольку Malwarebytes Endpoint Protection — комплексное решение для защиты от шпионского ПО, программ-вымогателей, атак нулевого дня, троянов и руткитов. Теперь вам не нужен целый набор инструментов, чтобы обеспечить кибербезопасность.

Malwarebytes Endpoint Detection and Response

Решение Malwarebytes Endpoint Detection and Response разработано в расчете на задачи обеспечения безопасности крупных и средних компаний. В дополнение ко всем функциям Malwarebytes Endpoint Protection оно включает ряд важных возможностей EDR:

- Детальная изоляция угроз для процессов, сетей и настольных ПК Windows
- Сбор подробной информации об угрозах для анализа и расследования
- Управляемый поиск угроз для обнаружения индикаторов взлома (IOC)
- 72-часовой откат после атак программ-вымогателей для рабочих станций Windows: вам никогда не придется платить выкуп, терять данные или заменять конечное устройство из-за подобной атаки
- Улучшенная защита протокола удаленного рабочего стола для блокировки взлома системы методом подбора паролей
- Функции обнаружения вредоносного ПО корпоративного класса с использованием машинного обучения для выявления аномалий поведения
- Низкий процент ложных срабатываний

Низкий уровень ложных срабатываний Endpoint Detection and Response, в числе прочего, защищает компании от проблем с органами, контролирующими использование персональных данных и требующих от организаций доказывать, что их оповещения не раскрыли личной информации, либо платить штрафы за ее предполагаемое раскрытие.

Оба решения — Malwarebytes Endpoint Protection и Malwarebytes Endpoint Detection and Response — работают с компьютерами и ноутбуками под управлением Windows и MacOS в любых сочетаниях. Также доступна защита серверов.

Плюсы комплексного решения: Malwarebytes и TeamViewer

Передовая защита конечных точек Malwarebytes сочетается с поддержкой удаленного подключения и удобством TeamViewer.

Удаленный доступ к конечным устройствам

Когда Malwarebytes обнаруживает угрозу, вы можете удаленно подключиться к конечному устройству с помощью TeamViewer, чтобы проверить его настройки и статус, а также предпринять любые действия для снижения риска, — и все это с единой платформы. Даже когда Endpoint Detection and Response изолирует взломанное устройство для защиты сети, вы все равно можете безопасно подключиться к нему удаленно с помощью TeamViewer.

Интегрированная панель управления

Та же интегрированная панель управления TeamViewer, которая служит для безопасного мониторинга конечных устройств, развертывания исправлений и удаленного доступа к ним, позволяет быстро развертывать, запускать и управлять Malwarebytes. Это повышает уровень осведомленности о ситуации.

Повсеместная поддержка сотрудников

TeamViewer позволяет легко и быстро развертывать Malwarebytes для офисных, удаленных, гибридно-удаленных и BYOD-групп любого размера.

Готовность к запуску

Malwarebytes интегрируется с вашей панелью управления TeamViewer: решение можно загрузить и запустить одним щелчком мыши. Написание специального кода для установки не требуется.

Безопасность

Шифрование данных и программ

Соединения TeamViewer защищены обменом закрытых/открытых ключей 4096 RSA и 256-битным сквозным AES-шифрованием сеанса. Эта технология основана на тех же стандартах, что и https/SSL, и соответствует современным стандартам безопасности. Обмен ключами также гарантирует полную защиту данных при передаче между клиентами. Это означает, что даже наши серверы маршрутизации не могут читать поток данных. Все программные файлы защищены с помощью технологии подписывания кода DigiCert.

Основные возможности

Предотвращение угроз нулевого дня

Бессигнатурный анализ полезной нагрузки и выявление аномалий позволяют превентивно выявлять и блокировать вредоносные программы, пытающиеся использовать скрытые уязвимости в ОС и приложениях конечных устройств организации, упреждая атаки нулевого дня.

Единая интеллектуальная система обнаружения угроз

Обнаруживайте угрозы более точными и «умными» способами с меньшим количеством ложных срабатываний благодаря профилированию угроз в Интернете, памяти, приложениях и файлах с помощью мониторинга поведения и машинного обучения.

Централизованное сканирование и исправление

Отслеживайте и поддерживайте состояние защиты устройств в одном отделе или на тысячах устройств одновременно: для выявления угроз и помещения устройств в карантин в режиме автоматического сканирования и применения исправлений потребуется всего несколько щелчков мышью на централизованной облачной консоли.

Упреждающая блокировка на основе поведения

Анализ поведения позволяет выявлять действия вредоносного ПО в режиме, близком к реальному времени, и автоматически блокировать угрозы — на сегодняшний день это один из самых эффективных методов упреждающей защиты.

Комплексное исправление

Подробная аналитика на базе ядра Linking Engine позволяет полностью и навсегда удалить как заражение, так и любые оставшиеся артефакты.

Полная защита в Интернете

Предотвращайте доступ пользователей к вредоносным сайтам и рекламе, мошенническим сетям и подозрительным ссылкам, а также загрузку неразрешенных программ и внесение несанкционированных изменений.

Эффективная интеграция и быстрое развертывание

Решения Malwarebytes Endpoint Protection и Endpoint Detection and Response полностью интегрированы с TeamViewer и готовы к удаленному развертыванию без сложной настройки.

Легкое масштабирование и настройка

Наше облачное решение можно масштабировать для поддержки организации любого размера и настроить для задач конкретного отдела, чтобы эффективно обнаруживать сложные угрозы, а затем быстро и последовательно реагировать на них.

Обзор лицензий

	Endpoint Protection	Endpoint Detection and Response
Компьютеры и ноутбуки Windows и Mac	✓	✓
Многовекторная защита Защита от угроз всех видов, включая программы-вымогатели, вредоносное ПО, атаки нулевого дня, рекламное ПО и вирусы. Уровни защиты: • Интернет • Усиление защиты приложений • Поведение приложений • Предотвращение атак • Анализ полезной нагрузки • Машинное обучение для обнаружения аномального поведения • Защита от программ-вымогателей	✓	✓
Исправление • Технология исправления Linking Engine • Очистка зараженных устройств	✓	✓
Установка и управление • Централизованное управление в облаке • Политики безопасности • Управление группами конечных устройств • Легкое развертывание из панели управления Endpoint Protection • Панели мониторинга угроз • Сканирование по требованию и по расписанию • Отчеты по запросу и автоматические отчеты • Уведомления по электронной почте • Поддержка SysLog	✓	✓
Системные режимы изоляции • Сеть • Процесс • Рабочий стол	✗	✓
Возможности EDR • Выявление подозрительных действий и уведомление о них • Детальная изоляция конечных устройств • Откат после атак программ-вымогателей	✗	✓

Дальнейшие шаги

Оцените сами, как работают решения Malwarebytes: протестируйте бесплатную пробную в течение 14 дней — без каких-либо обязательств.

Запросить бесплатную пробную версию

Изучите решения Malwarebytes, интегрированные с TeamViewer.

Подробнее

Остались вопросы?
Позвоните нам: **49-7161-60692-50**

Контакты

О компании TeamViewer

TeamViewer — ведущая глобальная платформа для удаленного подключения, соединяющая пользователей любых систем в любое время и в любом месте. Компания предлагает безопасный удаленный доступ, поддержку, контроль и функции совместной работы для подключенных к Интернету конечных устройств всех типов, помогая предприятиям любого размера в полной мере использовать свой цифровой потенциал. Решение TeamViewer активировано примерно на 2,5 миллиардах устройств, при этом до 45 миллионов из них подключены к сети одновременно.

Основанная в 2005 году в Гёппингене (Германия), TeamViewer является публичной компанией, акции которой котируются на Франкфуртской фондовой бирже. В офисах компании в Европе, США и Азиатско-Тихоокеанском регионе работают около 1350 человек.

Оставаться на связи

www.teamviewer.com