Trend Micro™

ENDPOINT APPLICATION CONTROL

Предотвращает выполнение нежелательных и неизвестных приложений

Организации все больше осознают, что традиционные ориентированные на сигнатурный подход антивирусы не обеспечивают адекватной защиты от современных угроз и целенаправленных атак. Это усугубляется тем, что ежедневно появляются сотни тысяч новых вредоносных программ, что крайне затрудняет защиту от всех потенциальных угроз. Без надлежащей защиты вы рискуете потерять конфиденциальные данные компании, которые находятся на рабочих станциях и серверах. Кроме того, конечные точки могут использоваться в качестве плацдарма для проникновения в сеть вредоносных программ. Это увеличивает необходимость защиты данных и машин от непреднамеренных нарушений пользователями политик безопасности или от несанкционированного проникновения и последующего выполнения новых нежелательных или вредоносных приложений.

Trend Micro Endpoint Application Control позволяет повысить защиту от вредоносных программ и целенаправленных атак, предотвращая запуск неизвестных и нежелательных приложений на корпоративных конечных точках. Благодаря сочетанию гибких динамических политик, возможностей создания белого и черного списков, а также обширного каталога приложений, AppControl значительно снижает уязвимость конечных точек к атакам. Для детальной оценки ситуации и ориентированной на пользователей визуализации информация доступна в единой панели управления Trend Micro™ Control Manager™ .

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Что защищает:

- Конечные точки
- Сервера
- Встроенные устройства и POS-терминалы

Защита от угроз:

- Уязвимые объекты
- Вредоносные программы (исполняемые файлы, библиотеки DLL, драйверы устройств, приложения из Windows® Store и другие)

КЛЮЧЕВЫЕ ФУНКЦИИ

Расширенная защита от вредоносного ПО, целенаправленных атак и угроз нулевого дня:

- Предотвращает потенциальный ущерб от нежелательных или неизвестных приложений — исполняемых файлов, библиотек DLL, приложений Windows App, драйверов устройств, панели управления и других фалов формата PE (Portable Executable — переносимые исполняемые).
- Предоставляет глобальную и локальную информацию об угрозах в реальном времени, основанную на данных о репутации файлов, полученных в результате корреляции файлов по глобальным данным.
- Взаимодействует с дополнительными уровнями безопасности, чтобы лучше сопоставлять данные об угрозах и останавливать больше угроз.
- Анализирует данные приложения и сравнивает их с более чем миллиардом записей о безопасных файлах (Trend Micro™ Smart Protection Network™).
- Интеграция с Trend Micro User Protection для защиты от вирусов, предотвращения вторжений, предотвращения потери данных, безопасности мобильных устройств и т. д.

Упрощенное управление для быстрой защиты

- Увеличивает удобство гранулированного управления благодаря панели управления, настраиваемой под нужды администратора.
- Использует интеллектуальные и динамические политики, которые позволяют пользователям устанавливать проверенные приложения на основе репутационных характеристик, таких как глобальная и региональная распространенность, а также возраст приложения.
- Обеспечивает детальную картину развития угрозы, используя данные с хоста, управление политиками, и агрегацию журналов. Control Manager позволяет предоставлять отчеты по разным срезам.
- Легко развертывается с использованием существующей защиты конечных точек OfficeScan или других сторонних инструментов развертывания.
- Классифицирует приложения и обеспечивает регулярные обновления для упрощения администрирования с помощью сертифицированной службы безопасного программного обеспечения Trend Micro (Certified Safe Software Service).

Подробные белые и черные списки блокируют неизвестные и нежелательные приложения

- Использует имя приложения, путь, регулярное выражение или сертификат для создания базового белого списка и черного списка.
- Содержит огромный список предпроверенных приложений, которые можно легко выбрать из каталога приложений Trend Micro (каталог регулярно обновляется).
- Обеспечивает возможность установки патчей / обновлений для приложений из белого списка, а также позволяет вашим программам обновления устанавливать новые исправления / обновления из надежного источника.
- Позволяет создавать белые и черные списки приложений для собственных и неклассифицированнных приложений.
- Обеспечивает беспрецедентную широту приложений и данных хороших файлов.

Соблюдение внутренних ИТ-политик помогает уменьшить юридические и финансовые обязательства

- Ограничивает использование приложений конкретным списком приложений, поддерживаемых продуктами предотвращения утечек данных (DLP) для конкретных пользователей или конечных точек.
- Собирает и ограничивает использование приложений для соблюдения лицензий на программное обеспечение.
- Позволяет заблокировать изменения в системе, чтобы обеспечить защитой рабочие станции конечных пользователей, предотвращая выполнение новых приложений.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- Защищает от пользователей или компьютеров, запускающих вредоносное ПО.
- Упрощенное развертывание при использовании совместно с OfficeScan.
- Предоставляет расширенные возможности для централизованного принудительного применения корпоративных политик с помощью Control Manager.
- Использует обширный каталог классифицированных приложений (проанализированные и сопоставленные данные об угрозах из миллиардов файлов в Trend Micro Smart Protection Network).
- Использует динамические политики, позволяющие пользователям устанавливать утвержденные приложения на основе многих репутационных переменных, таких как распространенность, региональное использование и зрелость ПО.

АРХИТЕКТУРА ПЛАТФОРМЫ

Управление Trend Micro Endpoint Application Control может масштабироваться до 20 000 пользователей на сервер и далее с помощью кластера серверов или нескольких серверов, управляемых Control Manager. В качестве встроенного программного приложения Endpoint Application Control интегрируется с другими решениями защиты от угроз Trend Micro для повышения общей защиты от вредоносных программ. Требуются два компонента:

- Сервер устанавливается на поддерживаемые платформы Windows и управляется через веб-браузер.
- Агент устанавливается на поддерживаемые платформы Windows.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

РЕКОМЕНДУЕМЫЕ МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К СЕРВЕРУ

Операционная система сервера:

- Microsoft Windows Server 2008 и 2008 R2 (x86/x64)
- Microsoft Windows Server 2012 и 2012 R2 (x86/x64)
- Microsoft Windows Server 2016 (x86/x64)
- (Опционально) IIS v7.0 или выше с модулями: CGI, ISAPI, ISAPI Extensions

Серверная платформа:

- Процессор: поколение Intel XEON E5-2695 v3 или выше
- Память: минимум 8 ГБ, рекомендуется 16 ГБ
- Пространство на диске: 500 ГБ

РЕКОМЕНДУЕМЫЕ МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К АГЕНТУ

Операционная система агента:

- Windows (x86/x64) XP
- Windows (x86/x64) Vista
- Windows (x86/x64) 7
- Windows (x86/x64) 8, 8.1
- Windows (x86/x64) 10
- Microsoft Windows (x86/x64) Server 2003, 2003 R2
- Microsoft Windows (x86/x64) Server 2008, 2008 R2
- Microsoft Windows Server 2012, 2012 R2
- Microsoft Windows Server 2016
- Windows Embedded Enterprise, POSReady 2009, POSReady 7, XPe, Standard 2009, Standard 7

Платформа агента:

- Процессор: 300 MHz Intel Pentium или эквивалентный
- ОЗУ: 512 МБ
- Пространство на диске: 350 МБ

Подробные требования доступны по ссылке:
http://docs.trendmicro.com/en-us/enterprise/endpoint-application-control/requirements.aspx

User Protection

является частью Trend Micro™ Smart Protection Suites™. Эти взаимосвязанные многоуровневые пакеты безопасности защищают ваших пользователей и их данные независимо от того, какое устройство они используют или где они работают. Smart Protection Suites сочетают в себе широкий спектр возможностей защиты конечных точек и мобильных устройств с несколькими уровнями безопасности электронной почты, совместной работы и шлюза. Кроме того, вы получаете возможность управлять защитой пользователей от различных векторов атак с единой панели управления, что дает вам полную картину безопасности вашей среды.

Trend Micro Control Manager

это централизованная панель управления безопасностью, которая обеспечивает последовательное управление безопасностью и полную видимость, управление политиками и отчетность по различным взаимосвязанным уровням безопасности от Trend Micro. Она также расширяет видимость и контроль на локальные, облачные и гибридные модели развертывания. Благодаря сочетанию централизованного управления и видимости всех пользователей улучшается защита, уменьшается сложность и устраняются избыточные и повторяющиеся задачи администрирования безопасности. Control Manager также предоставляет доступ к интерактивным данным об угрозах с помощью связанной защиты от угроз Trend Micro из локальной песочницы или Trend Micro™ Smart Protection Network™, которая использует глобальную информацию об угрозах для обеспечения безопасности в реальном времени из облака, блокируя угрозы до их реализации.

TREND MICRO™

Securing Your Journey to the Cloud