Trend Micro™

OFFICESCAN™

Безопасность конечных устройств от признанного лидера

Когда-то общая картина угроз была однозначно черно-белой, с четким делением на хорошее и плохое. Однако в наши дни все сложнее становится отличить хорошее от плохого, и организации все более критически рассматривают безопасность конечных устройств. Возникло понимание: уже недостаточно использовать только традиционные методы обнаружения угроз на основе сигнатур для защиты от программ-вымогателей и прочих неизвестных угроз, все чаще проникающих в системы. Технологии безопасности нового поколения часто являются узкоспециализированными, и необходимость развертывания нескольких средств защиты от вредоносных программ на одном конечном устройстве приводит к росту числа конфликтов между подобными продуктами. Кроме того, пользователи все чаще обращаются к корпоративным ресурсам из разных мест и с разных устройств (и даже из облачных сервисов), что еще больше усложняет ситуацию. Вам необходимо решение по обеспечению безопасности конечных устройств, предоставляющее комплексную защиту от всех типов угроз, от проверенного вендора, которому вы можете доверять.

Trend Micro™ OfficeScan™ применяет высокоточное машинное обучение в сочетании с различными методами защиты от угроз, чтобы устранить слабые места в обеспечении безопасности любых действий пользователя и любых типов конечных устройств. Система постоянно обучается, адаптируется и автоматически обменивается информацией об угрозах с другими системами в вашей среде. Такая комбинация защиты от угроз достигается за счет особой архитектуры, которая использует конечные ресурсы более эффективно, значительно превосходя конкурентные системы в плане экономии использования ЦП и сети.

OfficeScan является важным компонентом нашего универсального пакета **Smart Protection Suites,** который предоставляет еще больше возможностей в плане защиты шлюзов и конечных устройств, включая такие функции, как управление приложениями, предотвращение вторжений (защита от уязвимостей), шифрование данных конечных устройств, предотвращение утечки данных (DLP) и многое другое. Дополнительные решения Trend Micro расширяют вашу защиту от сложных атак с помощью методов исследования и анализа конечных устройств. Кроме того, сетевая «песочница» Deep Discovery быстро реагирует и доставляет конечным устройствам обновления сигнатур в реальном времени в случае обнаружения новых локальных угроз, что позволяет ускорить принятие мер защиты и уменьшить распространение вредоносного ПО. При этом данная сложная технология безопасности остается простой для пользователей вашей организации, благодаря централизованной системе мониторинга, управления и отчетности.

ЭТО ВСЕ МОЖЕТ БЫТЬ ВАШИМ

- **Усовершенствованная защита от вредоносных программ и программ-вымогателей:** Защита конечных устройств (в пределах корпоративной сети или вне ее) от вредоносных программ – троянских программ, вирусов-червей, шпионского ПО, программ-вымогателей – с функцией адаптации для защиты от новых угроз по мере их появления.
- **Объединенная защита от угроз:** OfficeScan интегрируется с другими средствами обеспечения безопасности в вашей локальной сети, а также с облачным центром исследования угроз Trend Micro, и оперативно доставляет конечным устройствам обновления от сетевой «песочницы» в случае обнаружения новых угроз, что позволяет ускорить принятие мер защиты и уменьшить распространение вредоносного ПО.
- **Централизованный мониторинг и управление:** При развертывании в составе Trend Micro™ Control Manager™ управление несколькими серверами OfficeScan осуществляется с помощью единой панели, что обеспечивает пользователю целостный мониторинг системы.
- **Интеграция мобильной безопасности:** Интегрируйте Trend Micro™ Mobile Security и OfficeScan с помощью панели управления Control Manager, чтобы централизовать управление безопасностью и развертывание политик на всех конечных устройствах; Mobile Security включает в себя защиту от угроз для мобильных устройств, управление мобильными приложениями, управление мобильными устройствами (MDM) и защиту данных.

Объекты защиты:

- Физические конечные устройства;
- Виртуальные конечные устройства (дополнительный компонент);
- Серверы и компьютеры под управлением Windows;
- Компьютеры Mac;
- POS-терминалы и банкоматы.

Защита от угроз:

- Высокоточное машинное обучение (до и во время выполнения);
- Поведенческий анализ (против вредоносных скриптов, инъекций, программ-вымогателей, атак на память и браузеры);
- Служба File reputation;
- Обнаружение вариантов;
- Проверка распространенности;
- Служба Web Reputation;
- Предотвращение использования эксплойтов (МСЭ узла, защита от эксплойтов);
- Блокировка командных серверов;
- Предотвращение утечки данных (модуль DLP);
- Контроль внешних устройств;
- Проверка по базе хороших файлов;
- Интеграция «песочницы» с системой обнаружения угроз.

Посмотрите, как мы все это объединили

ПРЕИМУЩЕСТВА

Максимальная безопасность XGen™

Комбинация высокоточного машинного обучения с другими методами обнаружения угроз обеспечивает всеобъемлющую защиту от программ-вымогателей и иных сложных атак.

- Ступенчатая фильтрация угроз с помощью наиболее эффективного метода на каждом этапе, что дает максимальный уровень обнаружения без ложных срабатываний.
- Синтез технологий без сигнатур, включая высокоточное машинное обучение, поведенческий анализ, обнаружение вариантов, проверку распространенности, контроль приложений, профилактику эксплойтов и проверку по базе хороших файлов, с другими методами, такими как использование служб Web Reputation, File Reputation, а также блокирование командных серверов (C&C).
- Компания Trend Micro первой реализовала высокоточное машинное обучение путем уникального анализа файлов не только перед их выполнением, но и в процессе работы для более точного обнаружения угроз.
- При этом техники подавления ошибок, включая проверки распространенности и по белому списку на каждом уровне, помогают снижать количество ложных срабатываний.
- Мгновенный обмен информацией о подозрительной сетевой активности и файлах с другими эшелонами безопасности предотвращает последующие атаки.
- Усовершенствованная защита от программ-вымогателей отслеживает подозрительные действия шифрования файлов на конечных устройствах, прекращает несанкционированные действия и даже восстанавливает потерянные файлы в случае необходимости.

Минимальное воздействие

Сокращает влияние на пользователя и издержки на управление.

- Простая и оптимизированная система безопасности применяет нужную технику обнаружения в нужное время, что минимизирует степень воздействия на устройства и сети.
- Всесторонний централизованный мониторинг состояния конечного устройства позволяет быстро отследить угрозы безопасности.
- Автоматический обмен информацией об угрозах безопасности между эшелонами защиты позволяет организовать единую линию защиты от возникающих угроз во всей организации.
- Активируйте удаленную защиту и соответствие требованиям безопасности с помощью технологии ретрансляции Edge, чтобы сотрудники могли работать за пределами корпоративной сети и подключаться к OfficeScan без VPN.
- Настраиваемые панели управления позволят гибко выполнять различные обязанности администратора.
- Круглосуточная поддержка Trend Micro позволяет быстро разрешить возникшую проблему.

Надежный партнер в области безопасности

Trend Micro разрабатывает инновации уже длительное время и предоставляет наиболее эффективные и действенные технологии безопасности. Мы всегда стремимся разрабатывать новые технологии для борьбы с будущими потенциальными угрозами.

- Более 25 лет опыта в разработке технологий безопасности.
- Защита более 155 млн конечных устройств.
- Нам доверяют 45 из 50 крупнейших международных корпораций.
- Компания Trend Micro заняла самую высокую позицию Лидеры в магическом квадранте Gartner в 2017 году для платформ защиты конечных устройств.

Ключевые сложности у современных предприятий:

- Возросшее количество угроз вредоносного ПО и программ-вымогателей;
- Необходимость единого решения для защиты от всех известных и неизвестных угроз на компьютерах под управлением Windows, Mac и виртуальных рабочих столах;
- Решения по обеспечению безопасности конечных устройств не обмениваются информацией, требуют больше времени на применение мер защиты и увеличивают нагрузку на управление;
- Угрозы от пользователей, работающих удаленно и обменивающихся информацией новыми способами — через облако и подобные системы;
- Эффективность ИТ-служб снижается из-за отсутствия интеграции средств защиты от сложных угроз и защиты данных.

> “Моей первой задачей было избавиться от серьезной нагрузки, которую предыдущее решение для защиты конечных устройств оказывало на наши системы», — заявил г-н Джеймисон. «Мне удалось сделать это с помощью OfficeScan... Затем я захотел развернуть систему безопасности, которая действительно работает. Заменив предыдущее решение, мы убедились, что технологии Trend Micro блокируют распространение заражений”

Брюс Джеймисон (Bruce Jamieson)
администратор сетевых систем
компании A&W Food Services of Canada

СОЗДАЙТЕ СОБСТВЕННУЮ СИСТЕМУ ЗАЩИТЫ КОНЕЧНЫХ УСТРОЙСТВ

Расширьте существующую систему защиты конечных устройств Trend Micro с помощью дополнительных модулей безопасности и вспомогательных решений:

Модуль предотвращения утечки данных (DLP)

Защита важных данных, полная прозрачность и контроль:

- Защита конфиденциальных данных в сети и за ее пределами, включая шифрование файлов перед их отправкой за пределы сети;
- Предотвращение утечки данных через облачные хранилища, USB-накопители, подключаемые мобильные устройства, соединения Bluetooth и другие каналы;
- Поддержка большого числа устройств, приложений и типов файлов;
- Помощь в соблюдении нормативных требований за счет улучшенного контроля и принудительного применения политик.

Модуль «Безопасность для Mac»

Дополнительный уровень защиты для клиентов Apple Mac в сети блокирует доступ к вредоносным сайтам и распространение вредоносных программ (даже если их целью не является операционная система Mac OS X):

- Снижает опасность проникновения угроз через Интернет, в том числе вредоносного ПО, нацеленного на компьютеры Mac;
- Интерфейс в стиле системы Mac OS X для удобства пользователей;
- Экономия времени и сил благодаря централизованному управлению на всех конечных устройствах, включая компьютеры Mac.

Модуль «Инфраструктура виртуальных рабочих столов (VDI)»

Консолидация средств защиты конечных устройств в рамках единого решения, охватывающего как физические, так и виртуальные рабочие столы:

- Определяет среду агента (физическая или виртуальная) и оптимизирует средства защиты и производительность с учетом ее особенностей;
- Экономит ресурсы узла, так как упорядочивает сканирования и обновления, вносит базовые образы и уже просканированные данные в белые списки.

Шифрование данных конечных устройств

Защита конфиденциальных данных с помощью шифрования информации на конечных устройствах, таких как компьютеры Windows и Mac, DVD-диски и USB-накопители, которые могут быть легко потеряны или украдены. Решение Trend Micro™ Endpoint Encryption обеспечит безопасность данных на требуемом уровне за счет полного шифрования дисков, шифрования отдельных папок и файлов, а также данных на съемных носителях:

- Защита неактивных данных с помощью ПО для полного шифрования дисков;
- Автоматизация управления данными за счет использования жестких дисков с функцией самошифрования;
- Шифрование данных в отдельных файлах, общих папках и на съемных носителях;
- Настройка детальных политик управления устройствами и данными;
- Управление функциями Microsoft Bitlocker и Apple FileVault.

Защита от уязвимостей

Stops zero-day threats immediately on your physical Мгновенное блокирование угроз «нулевого дня» на физических и виртуальных рабочих столах, а также ноутбуках как в сети, так и за ее пределами. Благодаря системе предотвращения вторжений на уровне конечного узла (HIPS) решение Trend Micro™ Vulnerability Protection защищает вас от известных и неизвестных уязвимостей до момента появления и установки соответствующего пакета исправлений. Защита распространяется на критически важные платформы, включая устаревшие операционные системы, такие как Windows XP:

- Устраняет угрозы заражения, блокируя уязвимости с помощью виртуальных исправлений;
- Сокращает время простоя из-за восстановления систем и экстренной установки исправлений;
- Позволяет устанавливать исправления в удобное время и на своих условиях;
- Обнаруживает уязвимости и сообщает о них, основываясь на идентификаторах CVE, MS или на тяжести уязвимости.

Контроль приложений на конечных устройствах

Усиливает защиту от вредоносных программ и направленных атак, блокируя запуск нежелательных и неизвестных приложений на компьютерах организации:

- Защищает пользователей и компьютеров от запуска вредоносных программ;
- Динамические политики уменьшают влияние управления и обеспечивают гибкость для активных пользовательских сред;
- Ограничивает набор приложений, которые можно установить в системе;
- Создает и актуализирует базы данных разрешенных и безопасных приложений на основе сведений об угрозах, полученных путем анализа миллиардов файлов.

Endpoint Sensor

Мониторинг состояния безопасности на конечных устройствах с учетом контекста, регистрация действий на уровне системы и формирования подробных отчетов, с помощью которых аналитики угроз могут оперативно оценить характер и масштаб атаки. С помощью настраиваемых средств обнаружения, аналитики и контроля Deep Discovery вы можете:

- выявлять и анализировать действия злоумышленников;
- мгновенно адаптировать систему защиты с учетом особенностей атаки;
- оперативно реагировать на угрозу до потери важных данных.

Trend Micro™ Control Manager™

Эта централизованная панель управления безопасностью обеспечивает согласованное управление, полный контроль и создание отчетов на нескольких уровнях интегрированной системы защиты Trend Micro. Она позволяет контролировать локальные, облачные и гибридные среды. Средства централизованного управления в сочетании с инструментами контроля пользователей улучшают защиту, снижают сложность и позволяют администратору системы безопасности избавиться от выполнения лишних и повторяющихся задач. Control Manager также обеспечивает доступ к оперативной информации из инфраструктуры Trend Micro™ Smart Protection Network™, которая использует облачные данные об угрозах со всего мира и в режиме реального времени обеспечивает информационную безопасность, блокируя угрозы до того, как они попадут на компьютеры клиентов.

СИСТЕМНЫЕ ТРЕБОВАНИЯ OFFICESCAN

МИНИМАЛЬНЫЕ РЕКОМЕНДУЕМЫЕ ТРЕБОВАНИЯ К СЕРВЕРУ

Серверная операционная система OfficeScan:

- Windows Server 2008 (SP2) и 2008 R2 (SP2) (64-разрядная версия);
- Windows Storage Server 2008 (32- и 64-разрядные версии), Storage Server 2008 R2 (SP1) (64-разрядная версия);
- Windows HPC Server 2008 и HPC Server 2008 R2 (64-разрядная версия);
- Windows MultiPoint Server 2010 и 2012 (64-разрядные версии);
- Windows Server 2012 и 2012 R2 (64-разрядная версия);
- Windows MultiPoint Server 2012 (64-разрядная версия);
- Windows Storage Server 2012 (64-разрядная версия);
- Windows Server 2016 (64-разрядная версия).

Серверная платформа OfficeScan:

Процессор: Intel Core 2 Duo (двухъядерный) с тактовой частотой 1,86 ГГц или более мощный;

Память: не менее 1 ГБ (рекомендуется 2 ГБ) с 500 МБ специально для OfficeScan (в системах семейства Windows 2008);

- не менее 2 ГБ с 500 МБ специально для OfficeScan (в системах семейства Windows 2010/2011/2012/2016);

Дисковое пространство: не менее 6,5 ГБ (7 ГБ при удаленной установке).

Платформа сервера ретрансляции Edge OfficeScan:

Процессор: Intel Core 2 Duo (двухъядерный) с тактовой частотой 2 ГГц или более мощный;
Память: Не менее 4 ГБ;
Дисковое пространство: Не менее 50 ГБ;
Операционная система: Windows Server 2012 R2
Сетевая карта:
1. 2 сетевые карты:
   - одна для локального соединения с сервером OfficeScan;
   - одна для внешнего соединения с агентами OfficeScan.
2. 1 сетевая карта с разделением портов для локальных и внешних соединений.

База данных:
1. SQL Server 2008 R2 Express (или более поздняя версия);
2. SQL Server 2008 R2 (или более поздняя версия).

МИНИМАЛЬНЫЕ РЕКОМЕНДУЕМЫЕ ТРЕБОВАНИЯ ДЛЯ АГЕНТА

Операционная система агента:

- Windows XP (SP3) (32-разрядная версия);
- Windows XP (SP2) (64-разрядная версия Professional);
- Windows Vista (SP1/SP2) (32- и 64-разрядные версии);
- Windows 7 (с пакетом SP1 или без) (32- и 64-разрядные версии);
- Windows 8 и 8.1 (32- и 64-разрядные версии);
- Windows 10 (32- и 64-разрядные версии);
- Windows 10 IoT Embedded;
- Windows Server 2003 (SP2) и 2003 R2 (32- и 64-разрядные версии);
- Windows Compute Cluster Server 2003 (схема «активный/пассивный»);
- Windows Storage Server 2003 (SP2), Storage Server 2003 R2 (SP2) (32- и 64-разрядные версии);
- Windows Server 2008 (SP2) (32- и 64-разрядные версии) и 2008 R2 (SP1) (64-разрядная версия);
- Windows Storage Server 2008 (SP2) (32- и 64-разрядные версии) и Storage Server 2008 R2 (64-разрядная версия);
- Windows HPC Server 2008 и HPC Server 2008 R2 (32- и 64-разрядные версии);
- Windows Server 2008/2008 R2 Failover Clusters (схема «активный/пассивный»);
- Windows MultiPoint Server 2010 и 2011 (64-разрядные версии);
- Windows Server 2012 и 2012 R2 (64-разрядная версия);
- Windows Storage Server 2012 и 2012 R2 (64-разрядная версия);
- Windows MultiPoint Server 2012 (64-разрядная версия);
- Windows Server 2012 Failover Clusters (64-разрядная версия);
- Windows Server 2016 (64-разрядная версия);
- Windows XP Embedded Standard (SP1/SP2/SP3) (32-разрядная версия);
- Windows Embedded Standard 2009 (32-разрядная версия);
- Windows Embedded POSReady 2009 (32-разрядная версия), Embedded POSReady 7 (32- и 64-разрядные версии);
- Windows 7 Embedded (SP1) (32- и 64-разрядные версии);
- Windows 8 и 8.1 Embedded (32- и 64-разрядные версии).

Платформа агента:

Процессор: Intel Pentium с тактовой частотой 300 МГц или эквивалентный
(в системах семейства Windows XP, 2003, 7, 8, 8.1, 10);

- Intel Pentium с тактовой частотой не менее 1,0 ГГц (рекомендуется 2,0 ГГц) или эквивалентный (в системах семейства Windows Vista, Windows Embedded POS, 32-разрядные версии Windows 2008);
- Intel Pentium с тактовой частотой не менее 1,4 ГГц (рекомендуется 2,0 ГГц) или эквивалентный (в системах семейства Windows 2016 и 64-разрядных версий Windows 2008).

Память: не менее 256 МБ (рекомендуется 512 МБ) со 100 МБ специально для OfficeScan (в системах семейства Windows XP, 2003, Windows Embedded POSready 2009);

- не менее 512 МБ (рекомендуется 2 ГБ) со 100 МБ специально для OfficeScan (в системах семейства Windows 2008, 2010, 2011, 2012);
- не менее 1 ГБ (рекомендуется 1,5 ГБ) со 100 МБ специально для OfficeScan (в системах семейства Windows Vista);
- не менее 1 ГБ (рекомендуется 2 ГБ) со 100 МБ специально для OfficeScan (в системах семейства 32-разрядных версий Windows 7, 8, 8.1 и Windows Embedded POSready 7);
- не менее 1,5 ГБ (рекомендуется 2 ГБ) со 100 МБ специально для OfficeScan (в системах семейства 64-разрядных версий Windows 7, 8, 8,1).

Дисковое пространство: Не менее 650 МБ.

Подробные требования см. на веб-сайте **docs.trendmicro.com**

> “В условиях нашей сети, которая охватывает всю страну, возможность управлять защитой мобильных устройств и компьютеров на базе одной платформы упрощает обеспечение безопасности всей сетевой среды и повышает производительность труда наших сотрудников”

Грег Белл (Greg Bell)
директор по ИТ
DCI Donor Services

Решение Trend Micro User Protection разработано на основе технологий XGen™, которые обеспечивают интеллектуальный подход, оптимизацию и единое решение для безопасности вашего предприятия.