

CA Anti-Spyware r8.1

CA ANTI-SPYWARE 8.1 ОБНАРУЖИВАЕТ И УДАЛЯЕТ ШПИОНЯЩЕЕ И НЕВИРУСНОЕ ВРЕДНОСНОЕ ПО, ОБЕСПЕЧИВАЯ ЗАЩИТУ ПАРКА ПК ОРГАНИЗАЦИЙ ЛЮБЫХ РАЗМЕРОВ ОТ СНИЖЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ, НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И КРАЖ ИНФОРМАЦИИ. CA ANTI-SPYWARE ПРЕДСТАВЛЯЕТ СОБОЙ ЛЕГКО РАСШИРЯЕМОЕ, ЦЕНТРАЛИЗОВАННО УПРАВЛЯЕМОЕ РЕШЕНИЕ, ПРЕДНАЗНАЧЕННОЕ ДЛЯ БОРЬБЫ СО ШПИОНЯЩИМ ПО, ХАРАКТЕРИЗУЕТСЯ ПРОСТОТОЙ РАЗВЕРТЫВАНИЯ И УПРАВЛЕНИЯ В КОРПОРАТИВНОЙ СРЕДЕ.

Основные характеристики

- Полное обнаружение и удаление шпионящего ПО;
- Превосходное управление
- Обновление антивирусной базы с сохранением пропускной способности сети
- Подробные отчеты
- Гибкая архитектура

Что нового в версии 8.1

- ГИП агента
- Защита в режиме реального времени
- Bandwidth Savings
- Pests Updates
- Поддержка дополнительных языков

Необходимость выявления шпионящего ПО

Компании всех размеров сталкиваются со всевозрастающей угрозой со стороны шпионящего ПО, инструментария хакеров, других невирусных, но вредоносных программ, а также надоедливых программ-паразитов, таких как ПО с показом рекламы.

Шпионящее ПО не просто ворует информацию о вычислительных ресурсах компании. Оно снижает быстродействие системы и эффективность работы в сети Интернет. Эти угрозы быстро распространяются и представляют серьезную опасность для безопасности и секретности конфиденциальных данных организаций во всем мире.

Обеспечение контроля за шпионящим ПО в сетевой корпоративной среде может представлять собой сложную задачу. В отличие от программ-вирусов, которые стараются нанести ущерб, шпионящее ПО может варьироваться от раздражающих программ-паразитов, например ПО с показом рекламы, до сложных секретных программных средств хакеров, которые могут вызвать серьезные проблемы для безопасности. Все чаще шпионящее ПО создается профессионалами с единственной целью: похищение ценных данных и конфиденциальной информации как можно более незаметно. Такое новое более опасное шпионящее ПО было названо "криминальным ПО".

Шпионящее ПО создает также проблемы, связанные с производительностью компьютеров. Например, проведенное группой специалистов по безопасности компании CA исследование показало, что один компьютер, на котором работают всего лишь два приложения с показом рекламы, может загружаться более 14 минут. В предположении, что сотрудники компании ежедневно перезагружают свои компьютеры и при этом работают пять дней в неделю в течение 50 недель, каждый сотрудник, имеющий зараженную машину, может терять около 60 часов в год за счет простоя ожидания загрузки компьютера.

Наличие шпионящего ПО в компании также снижает производительность штатных сотрудников IT-подразделения, отвечающих за работоспособность компьютеров компании. Ручное выявление и удаление нежелательных приложений может занять многие часы, поскольку каждый фрагмент шпионящего ПО может состоять из сотен или даже тысяч битов кода. С этим процессом регулярного удаления шпионящего ПО непосредственно связаны затраты времени, которые сотрудники IT-отдела должны потратить на удаление

шпионящего ПО вместо работы над более важными стратегическими бизнес-проектами.

Для эффективного решения сегодняшних проблем, связанных со шпионящим ПО, организациям требуется единое комплексное решение, оснащенное средствами обнаружения, полного удаления и централизованного управления. Являясь составной частью стратегии компании CA по интегрированному управлению борьбой с компьютерными угрозами, CA Anti-Spyware представляет собой комплексное решение, которое защищает конфиденциальную деловую информацию, повышает производительность ПК и се

тей и сокращает количество обращений в компьютерную службу помощи.

CA Anti-Spyware предлагает дополнительный уровень защиты, облегчающий контроль над одной из наиболее быстро растущих сегодня угроз в сети Интернет. CA Anti-Spyware базируется на опыте группы специалистов компании CA Security Advisor - одной из крупнейших в мире групп, занимающихся исследованиями в области шпионящего ПО - для круглосуточного мониторинга новых компьютерных угроз.

Снижение риска в корпоративной среде

ВСЕСТОРОННЕЕ СКАНИРОВАНИЕ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ. CA Anti-Spyware заранее отслеживает системные вызовы и перехватывает программу-шпиона до ее запуска, защищая компьютер пользователя от новых угроз. Можно также управлять расписанием сканирования и задавать объекты сканирования с консоли управления, что позволяет администраторам и конечным пользователям запускать процесс сканирования в заданное время или при входе в сеть. Процесс сканирования и обновления происходит в автоматическом режиме, что экономит время администраторов, затрачиваемое на решение проблем, связанных со шпионящим ПО.

ОБНАРУЖЕНИЕ И ПОЛНОЕ УДАЛЕНИЕ ШПИОНЯЩЕГО ПО. CA Anti-Spyware обнаруживает и удаляет шпионящий код из файлов и профилей/счетов пользователей, выявляя скрытые случаи заражения и обеспечивая комплексную защиту от шпионящего ПО. CA Anti-Spyware имеет одну из самых полных антивирусных баз в отрасли.

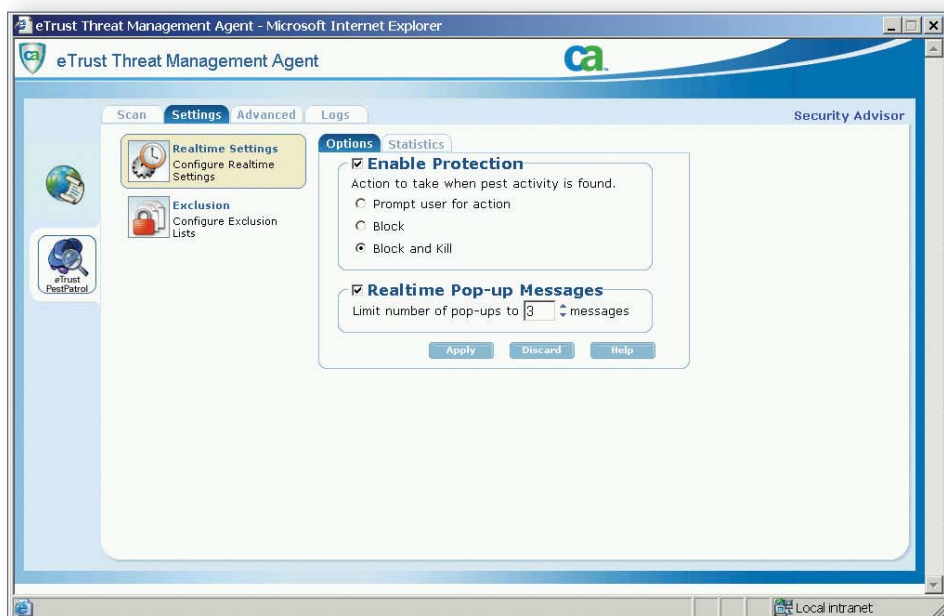
ПРЕВОСХОДНОЕ УПРАВЛЕНИЕ. CA Anti-Spyware обеспечивает всестороннюю защиту от шпионящего ПО посредством центральной консоли управления с веб-интерфейсом, которая позволяет осуществить простую установку, развертывание и администрирование программы в компании любого размера. С этой консоли администраторы могут осуществлять управление политиками сканирования и обновления, просматривать журналы регистрации и отчеты и предоставлять CA Anti-Spyware новым пользователям для централизованного управления безопасностью. CA Anti-Spyware и CA Anti-Virus можно управлять с одной консоли управления.

ЭФФЕКТИВНАЯ СВЯЗЬ С АГЕНТОМ. Связи между агентом приложения CA Anti-Spyware и основанной на Web-интерфейсе консолью управления инициируются агентом. Это позволяет агенту осуществлять регулярные "домашние звонки" на консоль управления, в ходе которых он сообщает свой статус и получает корректировку конфигурации, соответствующей новой политике, для активной борьбы со шпионящим ПО в режиме реального времени.

РИСУНОК А

CA Anti-Spyware предлагает простую и гибкую защиту в режиме реального времени от заражения шпионящим ПО.

CA ANTI-SPYWARE



ПОДДЕРЖКА CISCO NAC И MICROSOFT NAP. Подключаемый модуль CA Posture for Cisco NAC и продукт CA System Health Agent for Microsoft NAP позволяют получить важную информацию о текущей безопасности продуктов компании CA, установленных в сетях, защищенных Cisco NAC и Microsoft NAP.

ОБНОВЛЕНИЕ АНТИВИРУСНОЙ БАЗЫ ДАННЫХ С СОХРАНЕНИЕМ ПРОПУСКНОЙ СПОСОБНОСТИ СЕТИ.

На компьютер пользователя передаются уведомления об обновлении и новые файлы антивирусной базы для обеспечения защиты от самых последних версий угроз безопасности. Постепенное обновление DAT-файла снижает требования к пропускной способности сети, необходимой для поддержания безопасности на должном уровне.

УЛУЧШЕННОЕ РАЗВЕРТЫВАНИЕ В КРУПНЫХ КОРПОРАТИВНЫХ СРЕДАХ. Администраторы могут развертывать CA Anti-Spyware на компьютерах пользователей посредством программы разработки ПО любого стороннего разработчика, например Software Delivery от Unicenter, Systems Management Server (SMS) от Microsoft и других программ сторонних разработчиков. Это обеспечивает эффективное и безопасное развертывание приложения в крупных корпоративных вычислительных средах и максимальную отдачу от текущих инвестиций, вложенных в разработку ПО.

ПОДРОБНАЯ ОТЧЕТНОСТЬ. Для облегчения оценки угрозы можно создавать отчеты по рабочим станциям, дате/времени, приоритетам угроз безопасности и категориям вируса либо по конкретным вирусам. Отчеты по обнаруженным вирусам объединяются в единый журнал регистрации, ведущийся на выделенном сервере, что обеспечивает улучшенное управление и решение проблем.

ПРЕДУПРЕЖДЕНИЯ, ВЫДАВАЕМЫЕ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ. При обнаружении вредоносного кода CA Anti-Spyware выдает предупреждение, регистрирует событие и позволяет пользователю удалить этот код в режиме реального времени. Можно сконфигурировать автоматическую посылку сообщений с предупреждениями о вредоносном коде по электронной почте для решения специфических задач. Администратор может определить "безопасные списки" или файлы исключений определенных приложений, тонко настроенных IT-отделом или отдельным лицом во избежание подачи ложной тревоги.

ГИБКАЯ АРХИТЕКТУРА. CA Anti-Spyware построено на базе многоуровневой архитектуры с резервированием, которая допускает плавное масштабирование для управления большими группами пользователей ПО, предназначенного для борьбы с вирусами и вредоносным кодом, с единой консоли управления.

ДОПОЛНЯЕТ ТРАДИЦИОННЫЕ ТЕХНОЛОГИИ БЕЗОПАСНОСТИ И ПРЕВЕНТИВНЫЕ ТЕХНОЛОГИИ ПРЕДОТВРАЩЕНИЯ УГРОЗ. CA Anti-Spyware улучшает и расширяет защиту, обеспечиваемую как традиционными технологиями безопасности, так и превентивными технологиями предотвращения угроз, например антивирусными, антиспамовыми системами, межсетевыми экранами и системами обнаружения вторжений. CA Anti-Spyware специально разработано и протестировано в качестве дополнения к семейству антивирусных продуктов производства CA, включая CA Anti-Virus, CA SCM и CA HIPS, и обеспечивает многоуровневую защиту от компьютерных угроз.

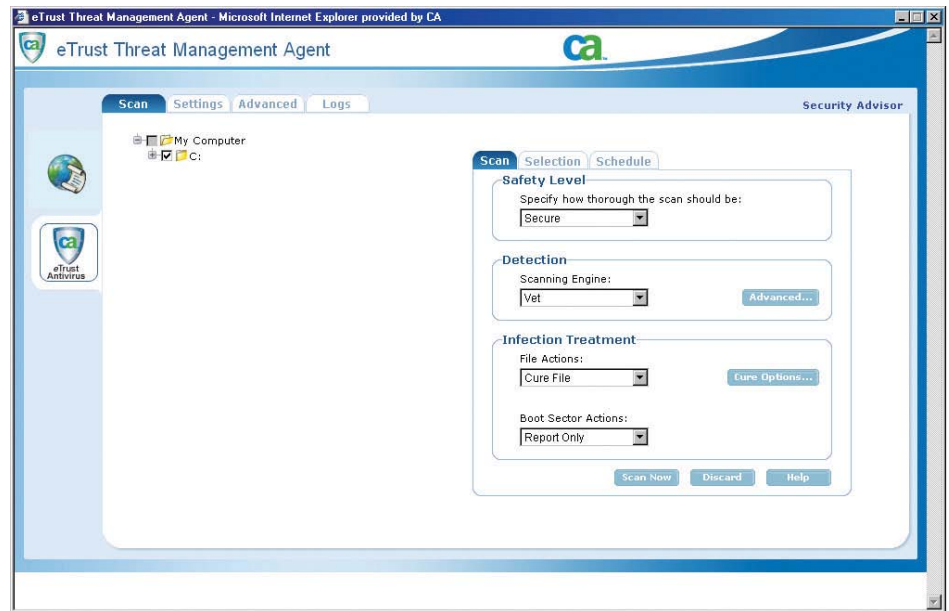
ОДОБРЕНО ЭКСПЕРТАМИ В ДАННОЙ ОБЛАСТИ. CA Anti-Spyware получил сертификат настольной антивирусной системы от West Coast Labs, независимой организации, которая проводит испытания продуктов, связанных с информационной безопасностью, на обнаружение троянов, программ-перехватчиков вводимой с клавиатуры информации и другого вредоносного софта разного рода.

CA SECURITY ADVISOR. CA Anti-Spyware поддерживается подразделением Security Advisor компании CA, которое служит надежным источником информации по безопасности для правительств, предприятий, образовательных учреждений и некоммерческих организаций с 1987 г. Штатными сотрудниками подразделения CA Security Advisor являются ведущие в отрасли исследователи, которые непрерывно отслеживают новые угрозы нарушения безопасности и разрабатывают процедуры борьбы с ними. Имея связь с разбросанными по всему миру центрами быстрого реагирования, CA Security Advisor проводит круглосуточные исследования компьютерных угроз и разрабатывает антивирусные базы данных, собирая их более чем из 400 источников с помощью своего запатентованного процесса для исследования, тестирования и контролирования компьютерных угроз.

РИСУНОК Б

Агент CA Anti-Spyware 8.1 обеспечивает результаты сканирования

АГЕНТ ANTI-SPYWARE



Что нового в версии 8.1

- **Графический интерфейс агента.** Опциональный графический интерфейс агента позволяет пользователям запускать процесс сканирования на выявление наличия шпионящего ПО и отслеживать его на своих рабочих станциях по мере необходимости в соответствии с политикой компании. Он дает возможность конечным пользователям отслеживать состояние защиты своих компьютеров в режиме реального времени, просматривать журналы регистрации, создавать и просматривать списки исключений и восстанавливать файлы, помещенные в карантин, в соответствии с политикой компании.
- **Защита в режиме реального времени.** Новые работающие в режиме реального времени функции CA Anti-Spyware отслеживают работу и сканируют все приложения и процессы по мере их загрузки для предотвращения запуска шпионящего ПО. Если компьютерная система уже заражена и шпионящее ПО работает к моменту запуска CA Anti-Spyware, по желанию пользователя можно остановить шпионящий процесс в памяти.
- **Поддержка дополнительных языков.** Помимо английского, французского, итальянского, немецкого, испанского и японского языков, CA Anti-Spyware 8.1 поддерживает бразильский португальский, традиционный китайский и упрощенный китайский языки.

Системные требования

Клиентский компьютер

- Pentium 150 или более мощный, 64 Мб свободного дискового пространства и 512 Мб свободной ОП
- Windows NT 4.0, SP6A или более поздний
- Windows 2000
- Windows Server 2003
- Windows XP Professional

Управляющий сервер

- Pentium 4, работающий на частоте 2.6 Мгц или более мощный, 10 Гб свободного дискового пространства и 1 Гб ОП
- Windows NT 4.0, SP6A или более поздний;
- Windows 2000 Server
- Windows 2003 Server
- Windows XP Professional
- Windows 2000 Workstation

Примечание: ОС Windows XP Professional и Windows 2000 Workstation не рекомендуется использовать вследствие их ограничения на десять одновременных соединений.

