

Как избежать остановок в работе и предотвратить ущерб от вредоносного ПО

Количество IT-угроз растет, они становятся все более разнообразными. Крайне важное значение имеет время, необходимое для обнаружения новых угроз и восстановления повреждений. Необходимо в кратчайшие сроки предотвратить потери производительности, вызванные вредоносным кодом, частично или полностью нарушившим работу систем.

Большинство атак нацелено на компьютеры неопытных пользователей, которые скачивают все типы программ, в том числе рекламное ПО, и открывают спамовые сообщения или сообщения, содержащие червей.

В результате, администраторы постоянно вынуждены устранять последствия атак. Оперативно решать эти проблемы можно только с помощью автоматической комплексной системы защиты.

Используйте полную защиту без снижения производительности ваших рабочих станций

Panda Security for Desktops – это идеальное решение для защиты рабочих станций от широко распространенных и мгновенно распространяемых вирусов и других угроз: спама, шпионов, руткитов, опасного или непродуктивного контента и фишинга, хакерских атак и вторжений.

В дополнение к непревзойденным способностям продукта в обнаружении и уничтожении, **Panda for Desktops** также выделяется своей высокой производительностью, сверхнизким потреблением системных ресурсов и минимальными затратами на сопровождение. Его административная консоль Panda AdminSecure минимизирует риск инфицирования для всех рабочих станций, терминалов и ноутбуков в Вашей компании, препятствуя атакам, которые используют уязвимости, и изолируя в карантине файлы и почтовые сообщения, передающие новые угрозы.

Стратегия многоуровневой защиты

Panda for Desktops защищает рабочие станции от вирусов и хакеров.



Основные выгоды

- Позволяет просто и централизованно управлять, внедрять, контролировать и определять политики безопасности.
- Позволяет **в режиме реального времени принимать решение**.
- **Защищает рабочие станции** на всех уровнях.
- **Контролирует поведение пользователей**, которые могли бы занести в сеть инфекции.
- **Повышает производительность** администратора и конечных пользователей.

Ключевые характеристики

- **Максимальная защита и минимальный риск инфицирования** со стороны вирусов, хакеров, руткитов и других угроз, благодаря эффективному обнаружению уязвимостей.
- **Немедленная реакция** на новые угрозы через сетевой **глобальный карантин**, полностью автоматические обновления **каждый час** и проактивные бюллетени.
- Новые **технологии TruPrevent™ (HIPS)**, предотвращающие воздействие неизвестных вредоносных программ путем блокировки подозрительных процессов и предотвращения атак отказа от обслуживания (DoS), а также переполнения буфера.
- **Фильтрация контента и защита от спама** для обнаружения и уничтожения потенциально опасного или отвлекающего контента.
- Содержит **Panda Malware Radar** - первый автоматизированный сервис аудита безопасности, который производит тщательные онлайн-сканирования Ваших IT-ресурсов для предоставления максимальной защиты от направленных атак, бот-сетей и прочих угроз.
- **Полный контроль** внутренних и внешних компьютеров при доступе как изнутри, так и снаружи локальной корпоративной сети (мобильные компьютеры).
- Быстрое и простое **внедрение и поддержка** системы.

Максимальная защита и минимальный риск инфицирования

Panda for Desktops защищает от атак хакеров, которые используют новые уязвимости, червей, распространяющихся с использованием техник социальной инженерии, кражи конфиденциальной информации со стороны нелояльных сотрудников, шпионов. Продукт также предлагает полную защиту от любых атак и вредоносного ПО, которое способно проникнуть через различные протоколы, приложения передачи сообщений (MSN Messenger, Yahoo Messenger или AOL Messenger), электронную почту и т.д. Он также позволяет Вам контролировать приложения, используемые сотрудниками, и защитить их от запуска опасного ПО.

Ежечасные обновления и глобальный карантин для подозрительных файлов

Panda for Desktops - это эффективное и стабильное решение, включающее зону централизованного карантина и ежечасные инкрементные обновления сигнатурного файла для предотвращения новым угрозам.

Технологии TruPrevent против неизвестных вирусов и вторжений

Технологии TruPrevent (HIPS) наблюдают за процессами, запущенными в данный момент, на предмет поиска вредоносного поведения. Они не только обнаруживают неизвестные вредоносные коды, но также блокируют их взаимодействие для предотвращения их запуска, и запрашивают "вакцину" в Panda для лечения и восстановления ПК с помощью технологии SmartClean2.

Panda for Desktops предоставляет интеллектуальный ответ благодаря эвристическому движку Genetic Heuristic Engine (предварительная классификация угроз до момента их запуска), автоматическому файерволу (глубокий анализ передаваемых пакетов данных на поиск вредоносных программ) и модулю обнаружения переполнения буфера, который наблюдает за доступом памяти.

Защита от спама и фильтрация контента

В дополнение к защите почтовых протоколов MAPI, POP3, SMTP и NNTP, **Panda for Desktops** содержит эффективный механизм защиты от спама, использующий правила, Байесовы шаблоны, списки и удаленное обучение для классификации спама, что позволяет пользователю классифицировать почту в Microsoft Outlook или Outlook Express.

Но встроенный спам-фильтр не в состоянии блокировать все типы опасного контента. По этой причине **Panda for Desktops** содержит защиту от фишинговых атак и опции фильтрации почты по его расширениям или MIME-типам.

Усиление технологий защиты

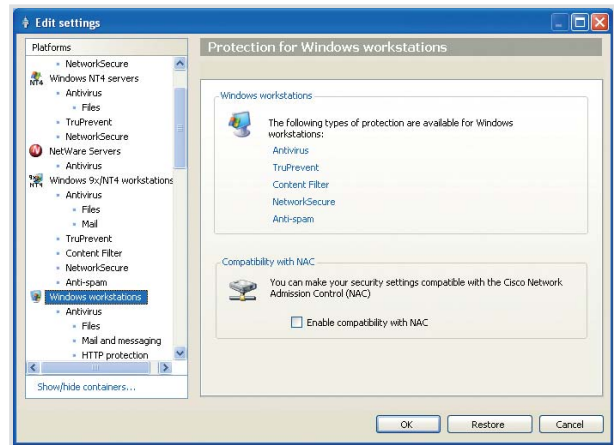
Для усиления защиты в **Panda for Desktops** встроен модуль NetworkSecure, который интегрирован с программами безопасности типа CISCO NAC. Он гарантирует контроль доступа через MAC-адреса, ограничивает риск кражи конфиденциальной информации, а также гарантирует то, что внешние сотрудники подключены к локальной сети с соблюдением правил безопасности.

Panda for Desktops, благодаря системе роуминга, сопровождает Вас повсюду, куда бы Вы ни пошли, даже если Вам необходимо обновить защиту из дома, отеля или офиса клиента, подключаясь для этого к корпоративному Extranet.

Быстрое и простое внедрение и сопровождение

Без Panda AdminSecure, консоли для управления **Panda for Desktops**, выполнение последовательной политики безопасности не могло

быть проще. Решение можно установить двумя способами: либо из консоли, используя IP-адреса или имена машин, либо вручную с использованием SMS или Tivoli. После установки продукта администраторы получают централизованный и глобальный обзор всей сети в режиме реального времени. Более того, они могут запускать удаленное сканирование по запросу и назначать распределяющий сервер с целью повышения отказоустойчивости. В целом, **Panda for Desktops** разработан с учетом возможности оптимизировать производительность компьютеров и потребление полосы пропускания.



Технические требования

Консоль Panda AdminSecure

Pentium II 266 МГц и выше.
ОЗУ: 140 МБ.
Жесткий диск: 140 МБ.
Internet Explorer 5.5.
Windows Installer 2.0.

Операционные системы: Windows 2000 / XP / XP 64-bits, Windows NT4 SP6 и Terminal Server, Windows 2000 Server SBS, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64-bits, Windows Vista 32-bits / 64-bits, Windows Server 2008 (32 и 64 bits).

Panda Security for Desktops

Pentium 300 МГц и выше.
ОЗУ Antivirus: 64 МБ. Рекомендуется 128 МБ.
ОЗУ Antivirus + TruPrevent: 128 МБ. Рекомендуется 512 МБ.
Жесткий диск: 200 МБ.
Outlook 4 и выше.

TP Technologies не поддерживаются на W95, XP 64-bits и Vista 64-bits.

Операционные системы: Windows 2000/Me (SP3), XP 32-bits/64 bits SP3, Vista 32-bits/64-bits SP2, WEPOS 1.1, Tablet PC и WEPOS Ready 2009.

"Все наши 1000 рабочих станций надежно защищены продуктами Panda Security".

Луис Валмики, Portucel, ПОРТУГАЛИЯ

Сертификаты Panda Security



Посетите www.pandasecurity.com

Получите Вашу демо-версию Panda Security for Desktops.

PANDA SECURITY | **20th** Anniversary 1990-2010