

Как защитить файловый сервер от атак и угроз до того, как они нанесут вред пользователям

Информация – это наиболее значимая ценность в любой организации, т.к. она крайне необходима для принятия любого решения. Когда для организации взаимодействия между членами коллектива информация доступна на сервере, присутствует серьезный фактор риска: ее потеря или кража, или даже невозможность ее использования для продолжения работы в том случае, если сервер атакуется или уже инфицирован.

Усиьте политики безопасности на ваших серверах и предотвратите ущерб от вредоносных программ

Panda Security for FileServers обеспечивает сохранность корпоративной информации, доступной в сети, от атак и других угроз. Данное высокопроизводительное решение с низким потреблением ресурсов защищает файловые серверы Windows от вредоносных программ, а также от уязвимостей, хакерских утилит и прочих угроз.

Panda Security for FileServers сочетает в себе быструю и наиболее усовершенствованную технологию для обнаружения неизвестных вредоносных программ с помощью технологий TruPrevent™. Эти эксклюзивные технологии, разработанные компанией Panda Security, содержат интеллектуальный движок для обнаружения атак типа "отказ от обслуживания" (DoS) и могут обнаруживать и анализировать открытые коммуникационные порты, приоритетно-захватные процессы и вредоносное поведение программ, которые не могут быть обнаружены антивирусными продуктами.

Продукт не допускает распространения массивных вирусных атак, шпионского и рекламного ПО, червей, троянцев... в ситуации, когда компьютеры имеют доступ к открытым сетевым ресурсам.



Основные выгоды

- Защищает файловые серверы на всех уровнях и гарантирует **целостность корпоративной информации**.
- Контролирует **поведение пользователя**, через которого инфекции могли бы проникнуть в сеть.
- **Увеличивает производительность** администратора и конечного пользователя.

Ключевые характеристики

- **Полноценный сканирующий движок последнего поколения** для защиты от вредоносных программ обнаруживает инфекции и сканирует на вирусы, черви, шпионы и другие угрозы на серверах.
- **Гибкое управление политикой и безопасные коммуникации**, обеспечиваемые мониторингом главных точек входа.
- **Перехват неизвестных вирусов и вторжений** с помощью новых технологий TruPrevent™ (HIPS).
- Полностью **автоматические ежедневные обновления** сигнатурного файла.
- **Оптимальная производительность** реактивной и превентивной защиты, чтобы минимизировать влияние на работу системы благодаря использованию специально разработанной серверной технологии.
- **Централизованное и удаленное администрирование** сети с различными серверными платформами для облегчения административных задач.

Полноценный движок для защиты от вредоносного ПО

Panda for File Servers предлагает для корпоративных файловых серверов надежную защиту от вирусов, червей, троянцев, руткитов, фишинга, следящих куков, шпионского и рекламного ПО, дозвончиков, шуток, хакерских утилит и прочих угроз безопасности. Включает в себя постоянную защиту HTTP, способность инспектировать открытые файлы в исключительном режиме, и мощный движок *Genetic Heuristic Engine (GHE)*, способный блокировать большинство новых неизвестных угроз.

Гибкое управление политиками и безопасные коммуникации

Для упреждения действий хакеров и вторжений, **Panda for File Servers** контролирует коммуникации и память, предотвращая переполнение буфера и основательно анализируя коммуникационные пакеты для обнаружения таких действий, как идентификация операционной системы, атаки типа "отказ в обслуживании", IP-спуфинг, MAC-спуфинг, сетевые вирусы...

В дополнение к **политикам безопасности по умолчанию** администратор может настроить доступ пользователя и приложений к системным ресурсам: файлы, регистрационные входы, COM-компоненты..., что позволяет усилить уровень безопасности в случае, например, фарминг-атак. В целом, FileSecure предотвращает инфицирование сервера из-за наличия к нему доступа со стороны внешнего персонала, который не имеет на своих компьютерах защиту Panda, также как и сотрудников без необходимых сертификатов физического доступа MAC-адреса для защиты от утечки информации.

Перехват неизвестных угроз

В дополнение к мощному движку по защите от вредоносных программ, **Panda for File Servers** содержит **технологии TruPrevent™ (HIPS)**, которые контролируют выполняемые процессы и осуществляют поиск программ с возможным нежелательным поведением, которые не могут быть обнаружены с помощью сигнатурного сканера и GHE.

Данная система способна обнаружить новые вредоносные программы, блокировать процесс, запретить его запуск (помещение файла на карантин) и защитить другие сетевые компьютеры от атаки. Благодаря технологии *SmartClean2* продукт автоматически лечит и восстанавливает сервер, значительно снижая риск инфицирования и возможного простоя.

Ежечасные автоматические обновления

Panda for File Servers может быть настроен так, что он будет автоматически каждый час проверять обновления сигнатурного файла и обновляться без вмешательства со стороны пользователя. Инкрементные обновления способствуют снижению использования полосы пропускания и сглаживанию коммуникационных пиков.

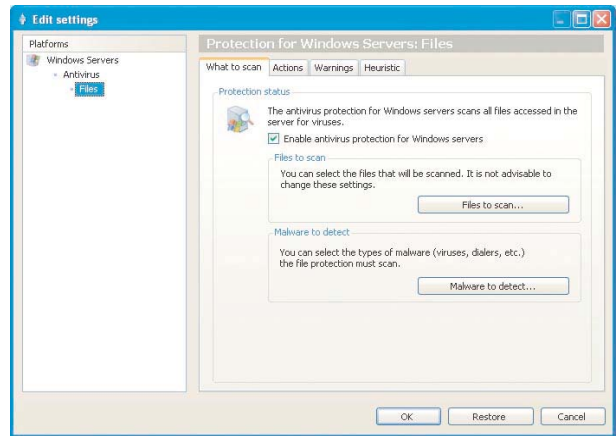
Оптимальная производительность

Panda for File Servers предоставляет высокопроизводительную защиту для файловых и принтерных серверов даже самых крупных компаний. Мультипоточное антивирусное ядро для параллельного сканирования допускает возможность использования серверного аппаратного обеспечения и способно распределять нагрузку между различными процессорами.

Продукт включает мощный кэш и систему *AutoTuning* для обеспечения стабильной работы как под независимыми, так и под кластерными серверными конфигурациями в 64-битных версиях операционной системы.

Удаленное централизованное управление

Panda for File Servers управляется удаленно и централизованно с помощью единой консоли **Panda AdminSecure**, через которую устанавливается вся защита, а инструментальная панель безопасности предоставляет информацию по уровню защиты серверов.



AdminSecure предоставляет обзоры, графические отчеты, предупреждения и т.д., также как и централизованный карантин, который позволяет управлять файлами с незавершенным лечением.

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 File Servers

Pentium 300 МГц и выше.

ОЗУ AV: 256 МБ.

ОЗУ AV+TP: 256 МБ. Рекомендуются 512 МБ.

Жесткий диск: 160 МБ.

Internet Explorer 5.5.

TruPrevent не поддерживается на 64-bits.

Операционные системы: Windows NT4 SP6 (Domain controller, SB Server, Terminal Server and cluster), Windows Server 2000 Domain Controller, StandAlone, Terminal Server, SB Server and cluster. Windows Server 2003 (32-bits и 64-bits) Enterprise Edition, SB Server, SP1, SP2 and cluster, Windows Server 2003 R2 (32-bits и 64-bits), Windows Server 2008 (32 и 64 bits), Windows SBS 2008 (32 и 64 bits).

"Процесс обновления сигнатурного файла, предоставленного Panda Antivirus, экономит нашему департаменту значительные средства и улучшает нашу репутацию перед пользователями."
Мистер Вернон Варнен, IT-менеджер, Wrexham Maelor Hospital, Великобритания.



Panda for File Servers можно приобрести отдельно или в составе **Panda Security for Business** или **Panda Security for Enterprise**.

Посетите www.pandasecurity.com

Получите Вашу демо-версию Panda Security for File Servers.

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