



Технические требования

Panda AdminSecure

Administration Server

Pentium III 800 МГц
ОЗУ: 256 Мб
Жесткий диск: 25 Мб + 120 Мб (DDBV) для работы в сети со 100 машинами.

Repository Server

Pentium III 800 МГц
ОЗУ: 128 Мб
Жесткий диск: 520 Мб

Communications Agent

Pentium 133 МГц
ОЗУ: 64 Мб
Жесткий диск: 40 Мб
Internet Explorer 5.5

Консоль

Pentium II 266 МГц или 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-bit, Windows Vista 32-bits/64-bits, Windows Server 2008 (32 и 64-bits).

Panda Security For CommandLine:

Pentium/Athlon и выше
Минимум ОЗУ: 128 Мб
Жесткий диск: 120 Мб
Жесткий диск 10 Мб
Операционные системы: Debian 4 и выше, Red Hat Enterprise 4 и выше, Mandrake 10.1/Mandriva 2006 и выше, Ubuntu 6.06 и выше, Fedora Core 5 и выше, CentOS 4.6 и выше, Windows NT/2000/XP/Windows Server 2003 (Enterprise Edition) /Vista

Panda Security For File Servers

Pentium 300 МГц или выше
ОЗУ AV: 256 Мб
ОЗУ AV+TP: 256 Мб. Рекомендуется 512 Мб
Жесткий диск: 160 Мб
TruPrevent не поддерживается в 64-bits

Операционные системы: Windows NT 4.0 с SP6 (Domain Controller, SB Server, Terminal Server и Cluster), Windows Server 2000 Domain Controller, StandAlone, Terminal Server, SB Server и Cluster, Windows Server 2003 (32-bits и 64-bits) Enterprise Edition, SB Server, SP1 и SP2 и cluster, Windows Server 2003 R2 (32-bits и 64-bits), Windows Server 2008 (32-bits и 64-bits), Windows SBS 2008 (32-bits и 64-bits)

Panda Security For Exchange

Exchange Server 2000/2003

Pentium II 500 МГц или выше
Минимум ОЗУ: 512 Мб для 2000 и 1 Гб для 2003
Жесткий диск: 200 Мб

Операционные системы: Windows 2003 Server (SP3), 2000 Advanced Server, Windows Server 2003 Enterprise Edition SP1 Server 2003 R2
Приложения: Microsoft Exchange Server 2000 SP1 или позднее, включая cluster, Exchange Server 2003 SP1 и выше

Exchange Server 2007

Intel processor с Intel Extended Memory 64 или AMD с AMD64 platforms.
ОЗУ: 2Гб минимум
Жесткий диск: 250 Мб
Операционные системы: Windows Server 2003 x64 или Windows Server 2003 R2 x64, Windows Server 2008 (Exchange 2007 SP1)
Приложения: Microsoft Exchange server 2007 или Exchange 2007 с SP1

Сегодня 95% компаний имеют в своей сети установленный антивирус, но 72% из них по-прежнему заражены вирусами.

Практически все организации малого и среднего бизнеса имеют установленное решение безопасности для защиты от вредоносных программ. Большинство из них чувствуют себя под защитой только потому, что у них установлен антивирус. Тем не менее, реальность такова, что очень высокий процент таких организаций по-прежнему заражен вредоносным ПО.

На первый взгляд может, конечно, показаться, что подобные инфекции не опасны для бизнеса, но согласно Gartner практически половине компаний малого и среднего бизнеса приходится отказываться от интернет-доступа по причине постоянных внешних вредоносных атак, приводящих к ощутимым потерям прибыли.

Следовательно, традиционной защиты уже недостаточно для удовлетворения потребностей безопасности. Вредоносное ПО теперь разрабатывается специально для того, чтобы оставаться незамеченным. Оно становится более комплексным, сложным и разнообразным, а во многих случаях перед ним ставятся совершенно определенные цели.

"Около 50% компаний малого и среднего бизнеса отключают внешний доступ к сети во время масштабных атак, потому что для многих из них это может обернуться крупной потерей прибыли".

Gartner: User Survey Analysis: IT Security Opportunities in the SMB Market, North America, 2007.

Решение: Panda Security for Business

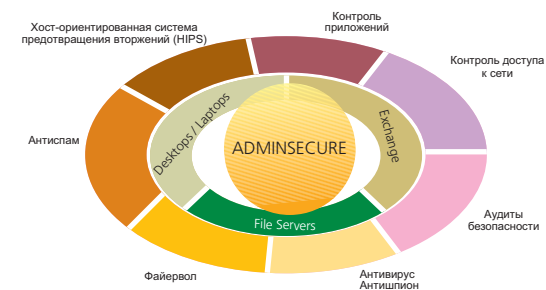
Panda Security for Business with Exchange обеспечивает **максимальную проактивную защиту** организации от угроз сегодняшнего и завтрашнего дня.

Основанный на комбинации наиболее продвинутых **проактивных технологий** (TruPrevent) и периодических **глубоких аудитов безопасности** (Malware Radar), продукт Panda Security for Business предлагает комплексную защиту от известных и неизвестных угроз.

Единая централизованная консоль управления (AdminSecure) позволяет администраторам **легко и просто** управлять всеми необходимыми модулями сетевой защиты. Она также дополнена интуитивно понятным мастером для распространения наиболее адекватной защиты на рабочие станции и сервера.

Panda Security for Business with Exchange содержит в едином наборе и **по единой цене** все модули защиты, необходимые организациям: хост-ориентированная система предотвращения вторжений, глубокий аудит направленных атак и скрытых угроз, управление приложениями и контроль сетевого доступа.

Решение основано на принципе **Коллективного разума**, который повышает эффективность обнаружений и максимизирует Вашу защиту от неизвестных угроз.



"Лучшим примером производителя, взявшегося за трудную задачу предоставления клиенту полного набора хост-ориентированных технологий предотвращения вторжений, является Panda Security с ее продуктом ClientShield, предоставляющим защиту по восьми из девяти параметров, описанных в нашем исследовании HIPS".
Gartner: How to Get Free Anti-spyware (or Antivirus) Protection.

Основные преимущества

- **Комплексный централизованный мониторинг всех компьютеров в сети.** Административный контроль AdminSecure позволяет администратору управлять глобальной безопасностью сети из одной или нескольких точек, оптимизируя производительность компьютера и позволяя использовать централизованную политику безопасности.
- **Эффективное решение безопасности.** Различные модули, включенные во все решения безопасности, предлагают каждой компании, независимо от ее размера, подходящий уровень безопасности в зависимости от структуры ее системы.
- **Гарантирует соблюдение корпоративной политики и оптимизирует производительность сотрудников.** Администратор может распространять политику безопасности на компьютеры и блокировать доступ к запрещенным приложениям или файлам с центральной консоли.
- **Упрощает управление рисками.** Корпоративные решения позволяют проводить автоматические глубокие проверки с целью обнаружения скрытого вредоносного ПО, которое могло остаться незамеченным в ходе других проверок.
- **Защищает важные ресурсы компании.** Проактивные технологии обеспечивают дополнительный уровень защиты от всех видов неизвестного вредоносного ПО, целевых атак и интернет-угроз.

Ключевые характеристики

- **Централизованная консоль все-в-одном,** позволяющая управлять всеми модулями защиты из единой точки. **Панель управления** обеспечивает защиту в реальном времени.
- **Самая продвинутая проактивная технология,** состоящая из системы предотвращения вторжений, проактивной защиты и поведенческого анализа.
- **Глубокий аудит безопасности и сервис лечения,** способные обнаруживать новые и самые совершенные скрытые угрозы.
- **Контроль сетевого доступа** для предотвращения подключения к Вашей сети зараженных, небезопасных или взломанных ПК, способных заразить Ваши файлы и данные.
- **Контроль приложений,** позволяющий администраторам полностью контролировать конечные точки и сетевые ресурсы.
- **Мультиуровневая и гибкая архитектура** для гетерогенных сетей, серверов и шлюзов.
- **Широкий ассортимент подробных отчетов** об обнаружениях, которые можно настраивать и периодически отправлять администраторам в автоматическом режиме.
- **Централизованно управляемый карантин,** который позволяет администраторам контролировать подозрительные файлы и принимать решения о дальнейших действиях, включая отправку в лабораторию PandaLabs для дальнейшего анализа.
- **Уведомления об инцидентах в реальном времени и мониторинг** статуса безопасности и производительности защиты.

