



Технические требования

**AdminSecure Administration Server:**

Pentium III 800 МГц (или быстрее); 256 Мб ОЗУ; Жесткий диск: 25 Мб + 120 Мб (База данных).

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

**AdminSecure Repository Server:**

Pentium III 800 МГц (или быстрее); 128 Мб ОЗУ; Жесткий диск: 250 Мб.

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

**Консоль AdminSecure:**

Pentium II 266 МГц; 64 Мб RAM; Hard disk: 140 Мб.

**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.

**Panda Security For Desktops:**

Pentium III 300 MHz (or faster). 64 MB RAM (128 MB if TruPrevent Technologies are enabled); Hard disk: 200 MB.

**Операционные системы:** Windows 2000 / ME / XP SP3 / XP SP3 64 bits, Windows NT4 (SP6) Windows Vista 32 bits/64 bits, Windows Vista (SP1). TruPrevent не поддерживается на Windows 95 and 64 bits.

**Panda Security For File Servers:**

**Windows Servers:**

Pentium 300 MHz (или быстрее); 256 Мб ОЗУ. Жесткий диск: 85 Мб

**Операционные системы:** Windows NT 4.0 SP6 Domain Controller, Small Business Server, Terminal Server и Cluster. Windows Server 2000 Domain Controller, Stand Alone, Terminal Server, Small Business Server and Cluster. Windows Server 2003 SP1 и SP2 (32bits и 64 bits) Enterprise Edition, Small Business Server и Cluster. Windows Server 2003 R2 (32 bits и 64 bits). Windows Server 2008, Server Core 2008, Small Business Server 2008. TruPrevent не поддерживается в 64 bits.

**Panda Security For Exchange:**

**For Exchange Server 5.5:** Pentium II 500 МГц (или позднее); 256 Мб ОЗУ; Жесткий диск: 250 Мб.

**Операционные системы:** Windows NT Server 4.0 (или позднее) с Service Pack 5 (или позднее) и Windows 2000.

**Приложения:** Microsoft Exchange Server 5.5 с Service Pack 3. Exchange cluster.

**For Exchange Server 2000/2003:**

**For Exchange Server 5.5:** Pentium II 500 МГц (или позднее); 256 Мб ОЗУ; Жесткий диск: 250 Мб.

**Операционные системы:** Microsoft Windows 2000 Advanced Server SP3 или позднее, Windows Server 2003/R2.

**Приложения:** Microsoft Exchange Server 2000 с SP 1 (или позднее) или Exchange 2003, включая cluster.

**For Exchange Server 2007:**

Intel EM64T или AMD64 platforms как минимум 2 Гб ОЗУ, как минимум 250 Мб пространства на жестком диске кроме Exchange 2007.

**Операционные системы:** MS Windows Server 2003 x64 или Windows Server 2003 R2 x64, Windows Server 2008 (только для Exchange 2007 SP1).

**Приложения:** Microsoft Exchange Server 2007 и Exchange 2007 SP1.

**Panda Security For Domino Servers:**

Pentium 133 МГц (или позднее); 128 Мб ОЗУ; Жесткий диск: 55 Мб Domino cluster.

**Операционные системы:** Windows NT Server 4.0 SP6a (или выше), Windows 2000, Windows 2000 Advanced Server и Windows Server 2003.

**Приложения:** Lotus Domino 4.5.x (или позднее). Domino Server 8 (32 bits).

**Panda Security For ISA Servers:**

**For Microsoft ISA Server 2000:**

Pentium II 300 Mhz или выше; ОЗУ: 256 Мб; Жесткий диск: 90 Мб.

**Приложения:** Windows 2000 Server, Advanced Server SP 1 (или выше) или Windows Server 2003/R2.

**Microsoft ISA Server 2004 (Standard and Enterprise Edition) и Microsoft ISA Server 2006 (Standard and Enterprise Edition):**

Pentium III 550 МГц или выше (4 CPUs на одном сервере). ОЗУ: 256 Мб; Жесткий диск: 180 Мб с NTFS.

**Операционные системы:** Windows 2000 Server, Advanced Server SP 4 (или выше) или Windows Server 2003/R2.

**Panda Security For Qmail, Panda Security For SendMail и Panda Security For PostFix:**

Pentium II 200 МГц (или выше); 64 Мб ОЗУ; Жесткий диск: 80 Мб, 90Мб для PostFix.

Угрозы наносят ущерб крупным организациям в размере 2,2% от их годового дохода, даже если установлено решение безопасности.

В сетях всех крупных организаций установлены традиционные решения безопасности, предназначенные для защиты сетей от вредоносного ПО. Благодаря таким решениям, компании в большинстве случаев защищены от массовых вредоносных атак, но они по-прежнему очень уязвимы для угроз нулевого дня и целевых атак.

Фактически, в 2007 г. угрозы нанесли крупным компаниям ущерб в размере 2,2% от их годового дохода. В результате инфекции наблюдается избыточная нагрузка на сетевые ресурсы и происходит отключение компьютеров, что вызывает значительную потерю производительности. Но чаще организации сталкиваются с менее заметными угрозами, например, с целевыми атаками, которые могут остаться незамеченными со стороны традиционных решений, чья работа основана на сигнатурном методе обнаружений. Производители антивирусов, которые продолжают защищать своих клиентов с помощью традиционных моделей, просто не в состоянии предложить им комплексную защиту по причине лавинообразного увеличения количества угроз.

Крупным организациям нужны комплексные решения, которые позволят им управлять рисками с помощью проактивных и превентивных методов. Принимая во внимание текущий сценарий действия вредоносного ПО, организациям необходимо адаптировать свою политику безопасности к современным требованиям.

Стратегия сетевой безопасности стремительно становится неотъемлемой частью бизнеса, поскольку она в состоянии защитить его от ущерба. Корректно подобранная стратегия безопасности может повысить прибыль компании за счет снижения рисков.

"Крупные организации держат под контролем клиентские вредоносные коды, но часто страдают от DOS-атак и серверного вредоносного ПО. Часто они тоже становятся объектами направленных атак..."  
Infonetics: The Cost of Network Security Attacks: North America 2007

Решение: Panda Security for Enterprise

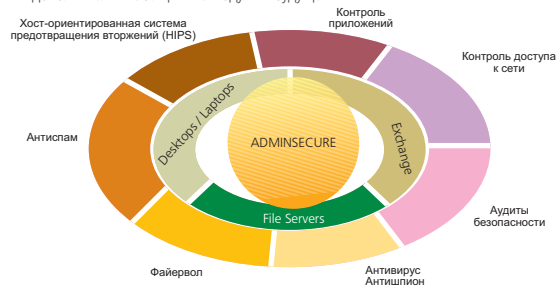
Panda Security for Enterprise предоставляет наиболее продвинутую проактивную защиту в мультиуровневой гибкой архитектуре, охватывающей все уровни сети. Его функционал включает сетевой доступ и контроль приложений.

Основанное на комбинации мультиуровневой проактивной защиты (TruPrevent) и периодических аудитах безопасности (Malware Radar), продукт предлагает комплексное превентивное решение для защиты от известных и неизвестных угроз.

Panda Security for Enterprise содержит защиту для рабочих станций, удаленных пользователей, файловых серверов, серверов электронной почты, серверов ISA и MTA.

Централизованная консоль (AdminSecure) объединяет информацию обо всех защитных модулях и позволяет администраторам управлять рисками за счет владения наиболее актуальной информацией об угрозах.

Panda Security for Enterprise – это единственный продукт, предлагающий все необходимые виды защиты в едином решении, в результате чего отпадает необходимость приобретать дополнительные защитные модули в будущем.



"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 автоматическое глубокие проверки с целью обнаружения скрытого вредоносного ПО, которое могло остаться незамеченным в ходе других проверок.
- Защищает важные ресурсы компании. Проактивные технологии обнаруживают 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, несанкционированных 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.

## Единая консоль управления

**Panda AdminSecure** - это централизованная консоль управления для Panda Security for Enterprise. Ее панель управления обеспечивает мониторинг в реальном времени, контроль безопасности и уровня риска всех сетевых систем: брандмауэров, веб-серверов, почтовых шлюзов, почтовых и файловых серверов и т.д.

**AdminSecure** адаптируется к структуре Вашей компании, позволяя Вам легко и просто устанавливать, обслуживать и контролировать защиту, установленную в Вашей сети, независимо от языка и количества компьютеров или платформ.

## Наиболее продвинутая проактивная технология

**Panda Security for Enterprise** содержит наиболее продвинутые и получившие признание проактивные технологии, использующие автоматические процессы, не требующие вмешательства пользователя. Продукт содержит генетический эвристический движок, поведенческое блокирование и поведенческое сканирование известных и неизвестных вредоносных кодов (технология TruPrevent).

## Аудит безопасности

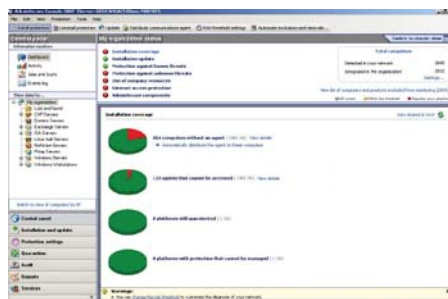
**Panda Malware Radar** - это автоматизированный аудит безопасности сети, в процессе которого выявляются зараженные объекты и угрозы, не обнаруженные традиционными решениями безопасности.

Основанный на принципе Коллективного разума, он дополняет и максимизирует Вашу защиту от скрытых угроз без инсталляции дополнительных компонентов и элементов инфраструктуры.

Malware Radar предоставляет автоматические проверки Вашей сети и подробные отчеты о результатах с рекомендациями по автоматизации задач лечения.

## Контроль сетевого доступа

Panda - это единственный производитель, в решения которого по умолчанию включена функция Контроля доступа к сети. Данная функция гарантирует, что в Вашу сеть не смогут проникнуть зараженные пользователи. Она просканирует каждый компьютер, пытающийся войти в сеть, чтобы определить, обновлен ли его антивирус (любой антивирус). Если ответ "нет", - он заблокирует доступ в сеть для такого компьютера.



## Антиспам на рабочих станциях и почтовых серверах

Panda Security for Enterprise содержит антиспамовую функцию для рабочих серверов и Exchange-серверов, что позволяет организациям повысить продуктивность и пропускную способность сети.

Антиспамовые движки, включенные в Panda Security for Enterprise, предлагают коэффициенты обнаружения более 95%.

## Контроль приложений

Использование некоторых приложений может представлять серьезную опасность для продуктивности организации. Благодаря функции контроля приложений администраторы смогут отслеживать приложения, использование которых запрещено.

## Всесторонняя фильтрация контента

Контент-фильтр проверяет информацию, содержащуюся в теле письма или в заголовке письма (например: "Тема:"), чтобы либо принять, либо отклонить сообщение.

## Подробные отчеты

Администраторы могут получать полные отчеты об активности своих сетей в любом удобном формате. Существует обширный перечень стандартных, предустановленных отчетов, но администратор всегда может сконфигурировать свои собственные отчеты.

Возможно использование опции регулярной отправки отчетов на заданные электронные адреса.

## Антивредоносная защита и фильтрация контента для Microsoft ISA servers

Гарантирует устойчивость Вашей политики безопасности. Останавливает распространение инфекций в локальных сетях. Сканирует все форматы файлов при получении и отправке. Это осуществляется при помощи Web-фильтра (ISAPI) и фильтра приложения через HTTP, SMTP и FTP (поверх HTTP).



## TruPrevent: Разумная поведенческая защита

Технологии TruPrevent входят во все продукты Panda Security как часть наиболее продвинутой проактивной защиты.

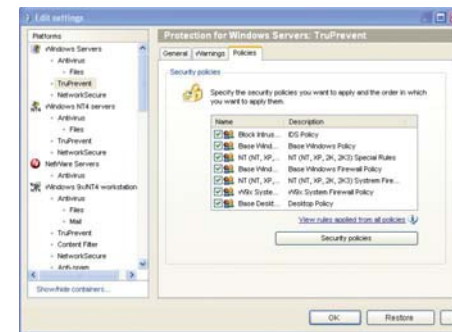
Благодаря своей способности обнаруживать поведенческие отклонения технология TruPrevent стала первой технологией, эффективно предотвращающей отказы сервисов, происходящие по причине вторжений и разных видов вредоносного ПО. Эта инновационная, высокоэффективная технология снижает риск заражения, а следовательно, и возможный ущерб.

Технология TruPrevent - это решение для рабочих станций и серверов, способное автоматически выявлять и блокировать черви, сетевые вирусы, шпионские программы и другие виды нового вредоносного ПО, которое сумело миновать другую защиту либо по причине недостаточной ее обновленности, либо из-за того, что решение, вместо того, чтобы предпринять нужное действие, просто уведомило администратора о возможной атаке.

Благодаря работе технологий TruPrevent, организации получают следующие преимущества:

- Снижение уровня риска, представляемого уязвимостями, и предотвращение распространения новых заражений, эксплуатирующих такие уязвимости до появления патча.
- Поддержание уровня безопасности Вашей сети за счет блокирования атак хакеров, краж конфиденциальной информации и инфекций, сгенерированных компьютерами, которые находятся под внешним управлением (удаленные сотрудники или пользователи, подключенные через Wi-Fi).
- Гибкая политика управления безопасностью, позволяющая доработать и усилить правила безопасности по всей сети для предотвращения кражи конфиденциальной информации нечестными сотрудниками.

Технологии TruPrevent Technologies - это прекрасное дополнение к антивирусу, обеспечивающее интеллектуальный слой защиты, который максимизирует способность обнаружения всех видов новых угроз и вторжений.



		Panda Security For Business	Panda Security For Business with Exchange	Panda Security For Enterprise
Console	AdminSecure	✓	✓	✓
Endpoint	Panda Security for Desktops	✓	✓	✓
	Panda Security for File Servers	✓	✓	✓
Mail	Panda Security for Postfix Servers		✓	✓
	Panda Security for Postfix		✓	✓
	Panda Security for Qmail			✓
	Panda Security for Sendmail			✓
Gateway	Panda Security for ISA Servers			✓
TechTools	Panda Security for Commandline	✓	✓	✓