Dr.WEB®
с 1992

Защити созданное

Сравнение функционала продуктов, предназначенных для защиты рабочих станций Windows

125124, Россия, Москва,
3-я улица Ямского поля,
вл. 2, корп. 12а

Телефон:
+7 (495) 789-45-87
Факс:
+7 (495) 789-45-97

www.drweb.com
www.av-desk.com
www.freedrweb.com
www.drweb-curenet.com
pda.drweb.com
estore.drweb.com

Dr.WEB®
с 1992

Таблица функционала продуктов

Функционал	Dr.Web Security Space 6.0	Dr.Web для Windows Server 6.0	Kaspersky Internet Security 9.0 /Антивирус Касперского 6.0 для Windows Workstations	ESET NOD32 Smart Security Business Edition 4.2	Symantec AntiVirus Corporate Edition	VirusScan Enterprise 8.5i	Agnitum Outpost Security Suite 2009
Компоненты продукта							
Консольный сканер	Dr.Web Консольный сканер для Windows	✗	✓	✗		✓	✗
Сканер с графическим интерфейсом	Dr.Web Сканер для Windows		✓	✓	✓	✓	✓
Антивирусный монитор	SpIDer Guard для Windows		✓	✓	Проверка при копировании, перемещении, открытии и обращении к файлу	✓	✓
Почтовый монитор	SpIDer Mail для рабочих станций Windows	✗	✓	✓	Защита Lotus Notes и Microsoft Exchange/ Microsoft Outlook	Защита Microsoft Outlook and Lotus Notes	✓
Родительский контроль	✓		✗	✗			
Проверка ссылок	✓	✗	✓	✗			✗
Файервол	В версии Pro		✓	✓		✓	✓
Самозащита	✓		✓	✓			✓
Возможность настройки каждого модуля по отдельности	✓		✓	✓	✓		✓
Возможность создания диска аварийного восстановления системы	Отдельный продукт		✓	SysResque	✗	✗	✗

Dr.WEB®
с 1992

Основные возможности продуктов							
Защита почтовых сообщений							
Антивирусная проверка почты	✓		✓	✓	✓	✓	✓
Антиспам проверка почты	✓		✓	Только в Smart Secutity	✗	✗	Только в Outlook и TheBat!
Обработка почтовых протоколов POP3/SMTP/IMAP4	✓		✓	✓/✗/✗	✓/✓/✗**	н/д	✓
Обезвреживание почтовых вирусов до получения писем почтовым клиентом с сервера или до получения письма почтовым сервером	✓		✓		н/д	✗	✓
Возможность отключения проверки почтового трафика некоторых программ	✓		MS Exchange	✓	✗	✗	Через HIPS
Возможность автоматического удаления писем на сервере по протоколу IMAP	✓		✗	✗		✗	✗
Отсутствие необходимости обучения антиспама	✓	✗	✗	✗			✗
Отсутствие необходимости использования дополнительных баз для работы антиспама	✓		✗				✗
Обработка протоколов новостей (NNTP)	✓		✓	✗	✗		✗
Ведение белых и черных списков отправителей почтовых сообщений	✓		✓	✗	✗	✗	✓
Выбор типа действий, применяемых к почтовым сообщениям, включая возможность модификации поля subject	✓		✓	✓	✗	✓/✗	✗
Задание списка проверяемых портов	✓		✗	✓			✗

Dr.WEB®
с 1992

Защита интернет-трафика							
Антивирусная проверка входящего и исходящего http-трафика	SpIDer Gate, Файервол	✗	Веб-Антивирус	✓			Веб-Антивирус
Возможность создания собственных правил	В версии Pro		✓	✓		✓	✓
Режим обучения	✓		✓	✓			✓
Фильтрация по MAC-адресам	✓		✗				✗
Задание списка проверяемых портов	✓	✗	✓	✓		✓	✓
Возможность блокирования выполнения скриптов, расположенных на веб-сайтах	✗	✓	✓	✗			✓
Регламентирование работы сетевых приложений	✓		✓	Только указывая браузеры, которые будут проверяться	✗		✓
Ведение белых и черных списков адресов сети Интернет	✓	✓	✓	✓	✗		✓
Родительский контроль							
Блокировка доступа к файлам и папкам	✓	✗	✗	✗		✓	✗
Ограничение доступа к локальным ресурсам сети	✓	✗	✗	✗	✗		На уровне файрвола
Ограничение доступа к ресурсам сети	✓	✗	✓	На уровне файрвола	✗		На уровне файрвола
Ограничение доступа к сменным носителям	✓	✗	✓	✓			✗
Защита работы приложений							
Защита критически важных процессов от изменений	✓	✓		✓		✓	✓
Защита файлов приложений (в том числе настроек) от изменений	✓	✓		✓		✓	✗
Создание списков доверенных приложений, трафик которых не будет проверяться	✓	✗		С вер. 4.2			

Dr.WEB®
с 1992

Возможности установки, обновления и запуска проверки						
Установка на зараженную систему без предварительного лечения системы	✓	✗	✗	✗	✗	✗
Возможность автоматического обновления через Интернет	✓	✓	✓	✓	✓	✓
Возможность обновления с HTTP- или FTP-серверов, локальных или сетевых каталогов	✓	✓	✓	✓	✓	✓
Возможность настройки параметров соединения	✓	✓	✓		✓	✓
Возможность обновления вручную	✓	✓		✓		✗
Возможность автоматического запуска при загрузке операционной системы	✓	✓	✓	✓	✓	✓
Возможность запуска процессов антивирусной проверки вручную, автоматически, по заранее составленному расписанию	✓	✓	✓	✓	✓	✓
Возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке	✓	✗	✗	✗	✗	✗
Возможность настройки заданий различного типа	✓	✓	✓	✓	✓	✗
Возможности обнаружения и удаления вредоносных объектов						
Возможность обнаружения и удаления активных (запущенных и выполняющихся в момент проверки) и пассивных вредоносных программы следующих типов: ▪ почтовые и сетевые черви; ▪ руткиты; ▪ файловые вирусы; ▪ троянские программы; ▪ бестелесные и стелс-вирусы; ▪ полиморфные вирусы; ▪ макро-вирусы и вирусы, поражающие документы MS Office; ▪ скрипт-вирусы.	✓	✓	✓	✓	✓	✓

Возможность обнаружения неизвестных вирусов	✓	✓	✓	✓	✓	✓
Возможность обнаружения и удаления вирусов, скрытых под неизвестными упаковщиками	FLY-CODE	✗	✗	✗	✗	✗
Возможность проверки оперативной памяти, в том числе на наличие руткитов и скрытых процессов	✓	✓	✓	✓	✓	✓
Возможность проверки загрузочных секторов всех дисков	✓	✓	✓	✓	✓	✗
Мониторинг попыток записи в загрузочный сектор	✓	✗	✓	✓		✗
Возможность проверки объектов автозапуска	✓	✓	✓			✓
Возможность проверки сменных носителей информации	✓	✓	✓	✓	✓	✓
Возможность проверки сетевых дисков	✓	✓	✓		✓	✓
Возможность проверки логических дисков	✓	✓	✓		✓	✓
Возможность выбора типов объектов, от которых будет осуществляться защита	✓	✓	✓	✓	✓	✗
Возможность проверки почтовых форматов	✓	✓	✓	✓	✓	✓
Возможность проверки файлов и каталогов, включая упакованные и находящиеся в архивах любой вложенности	✓	✓	✓	✗ (до десятого уровня вложенности)	✓	✓
Возможность проверки скриптов, включая VB-Script, Java Script	✓	✓			✓	✓
Наличие возможности мониторинга действий запущенных процессов и дисковых обращений	✓	✓	✓		✓	✓
Кеширование проверяемых файлов	✓			✓	✗	

Возможности проведения проверки						
Возможность выбора типа проверки (проверять все файлы, заданные файлы, файлы «по формату», файлы по заданному списку расширений, файлы по заданному списку масок)	✓	✓	✓	✓	✓/✗/✓/✗	✓/✗/✓/✗
Возможность быстрой/полной/выборочной проверки системы	✓	✓	✗/✓/✓	✗/✓/✓	✗/✓/✓	✓
Возможность задания папок и файлов, исключенных их проверки	✓	✓	✓	✓	✓	✗
Возможность выбора действий для зараженных, подозрительных объектов и объектов другого типа, включая лечение, переименование, перемещение и удаление	✓	✓	Выбирается уровень очистки, а не действия	✓****	✓	✗
Возможность задавать варианты действий над обнаруженным вредоносным объектом, если первоначальное или последующее действие невозможно	✓	✓	✗	✓	✓	✗
Возможность выбора действий для зараженных архивов	✓		✓		✗	✗
Возможность выбора действия для каждого зараженного объекта	✓	✓	✓		✓	✓
Проверка упакованных файлов и архивов	✓	✓	✓	✓	✓	✓
Возможность проверки без ограничения на уровень вложенности проверяемых объектов	✓	✓	✓	✗		✗
Возможность ограничения длины распакованного файла, подлежащего проверке	✓	✓	✓	✗	✗	✗
Возможность ограничения степени сжатия файла в архиве, подлежащего проверке	✓	✗	✓	✓	✗	✗

Сканирование альтернативных потоков данных (ADS) NTFS			✓			✗
Отсылка образцов на анализ	✓	✓	✓	✓	✓	Данные о приложениях
Запуск проверки по правому клику мышки	✓				✓	✗
Методы обнаружения вредоносных объектов						
Эвристический анализатор	✓	✓	✓	✓	✓	✓
Дополнительные технологии обнаружения вредоносных объектов, помимо сигнатурного метода и эвристического анализа	✓	✗	✓	✗	✗	✗
Возможности настройки						
Настройка через контекстное меню	✓	✓				✗
Настройка через главное окно приложения	✗	✓	✓		✓	✓
Настройка через окна параметров приложений	✓	✓	✗	✓		✓
Возможность возврата к настройкам по умолчанию		✓	✗	✗	✗	✓
Возможность оптимизации производительности работы						
Возможность отложенной проверки файлов, открываемых на чтение	✓		✗	✗	✗	✗
Многопоточная проверка файлов	✓	н/д	Для антиспама			
Возможность выбора приоритета сканирования	✓		✗	✓	✓	✗
Наличие функций самозащиты						
Защита работы собственных модулей от сбоев	Dr.Web SelfPROtect	✓	✗			✓
Возможность автоматического восстановления собственных модулей	✓		✗			

Защита от вредоносных программ и случайного изменения для всех своих объектов, в том числе, критических файлов, процессов	✓	✓	✗		✓	✓
Защита доступа к приложению с помощью пароля (всем операциям, либо их части)	✓	✓	✓	✓	✓	✓
Защита системного ядра	✓	✓	✗			
Возможности отчетов						
Наличие статистики работы приложения	✓	✓	✓	✓		✓
Возможность регистрации времени события, объекта проверки и типа воздействия	✓	✓	✓			✓
Возможность изменения уровня детализации отчетов	✓	✓	✓			✓
Возможность ограничения размеров файлов отчетов	✓	✓	✓		✓	✓
Индикация работы приложения через значок в системной панели	✓	✓	✗			✓
Индикация состояния защиты через индикаторы защиты	✓	✓	✗			
Просмотр статуса работы компонентов	✓	✓	✓			✗
Локализация						
Локализованная версия программы на русском языке	✓	✓	✓			✓
Руководство по эксплуатации на русском языке	✓	✓	✓	✓	✗	✓
Контекстно-чувствительная справка на русском языке	✓	✓	✓		✗	✓
Техническая поддержка на русском языке	✓	✓				✓

Достоинства и недостатки продуктов

Главным преимуществом персональных продуктов компании Доктор Веб версии 6.0 перед соответствующими продуктами Лаборатории Касперского являются:

- наличие дополнительных технологий обнаружения вредоносных объектов;
- наличие возможности автоматического удаления писем на сервере по протоколу IMAP;
- отсутствие необходимости обучения антиспама;
- наличие возможности фильтрации по MAC-адресам;
- возможность задания правил для родительских процессов;
- наличие расширенных возможностей родительского контроля, включая блокировку доступа к файлам и папкам, а также ограничение доступа к локальным ресурсам сети;
- существенно больший уровень самозащиты;
- наличие возможности установки на зараженную систему без ее предварительного лечения;
- возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке.

Главным преимуществом персональных продуктов компании Доктор Веб версии 6.0 перед соответствующими продуктами Agnitum являются:

- существенно лучший антивирус, обеспечивающий полный контроль за состоянием операционной системы;
- наличие дополнительных технологий обнаружения вредоносных объектов;
- лучший уровень проверки почтовых сообщений;
- наличие антиспама;
- наличие функций родительского контроля;
- существенно больший уровень самозащиты;
- наличие возможности установки на зараженную систему без ее предварительного лечения;
- возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке;
- возможность настройки заданий различного типа.

Системные требования сравниваемых продуктов

Системные требования для Dr.Web Security Space Pro

- Операционная система Windows 2000 SP4, Windows XP, Windows Vista, Windows 7. Поддерживаются 32- и 64-битные версии;
- процессор с системой команд i686 и старше;
- оперативная память – не менее 512 МБ.

Опущенные требования к конфигурации совпадают с таковыми для соответствующих операционных систем.

Системные требования для Антивируса Касперского 6.0 для Windows Workstations MP4

Для операционных систем Microsoft Windows 2000 Professional SP4, Windows XP Professional SP2, Windows XP Professional x64 SP2:

- процессор Intel Pentium 300 МГц 32-bit (x86) / 64-bit (x64);
- 256 МБ свободной оперативной памяти;
- 300 МБ свободного места на жестком диске.

Для операционных систем Microsoft Windows Vista SP1, Windows Vista x64 SP, Windows 7, Windows 7 x64:

- процессор Intel Pentium 800 МГц 32-bit (x86) / 64-bit (x64);
- 512 MB свободной оперативной памяти;
- 300 МБ свободного места на жестком диске.

Системные требования для ESET Smart Security Business Edition 4.2:

Для операционных систем Windows 2000, 2000 Server, XP, 2003 Server:

- процессор 400 МГц, 32-разрядный (x86) или 64-разрядный (x64);
- 128 Мб оперативной памяти;
- 130 Мб свободного места на жестком диске.

Для операционных систем Windows 7, Vista, Windows Server 2008:

- процессор 1 ГГц, 32-разрядный (x86) или 64-разрядный (x64);
- 512 Мб оперативной памяти;
- 130 Мб свободного места на жестком диске.

Outpost Security Suite Pro

Windows 2000 SP4, Windows XP, Windows Server 2003 или Windows Vista:

- процессор: 450 МГц Intel Pentium или совместимый;
- память: 256 Мб 2003;
- дисковое пространство: 100 Мб.

Symantec AntiVirus

Требования для установки клиента Symantec AntiVirus зависят от типа защиты, установленной на компьютере. Требования к дисковому пространству зависят от того, какие функции и компоненты устанавливаются.

Symantec AntiVirus (антивирусный клиент для 32+разрядных компьютеров):

- Windows 98/98 SE/Me; Windows NT 4.0 Workstation/Server/Terminal Server с пакетом обновления 6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Home/Professional/Tablet PC; Windows Server 2003 Web/Standard/Enterprise/Datacenter;
- не менее 32 Мб оперативной памяти;
- 55 Мб дискового пространства;
- обновление базового сертификата (Windows 98/98 SE).

Клиенты Terminal Server, подключаемые к компьютеру с антивирусной защитой, дополнительно предъявляют следующие требования:

- клиент Microsoft Terminal Server RDP (Remote Desktop Protocol);
- клиент Citrix Metaframe (ICA) 1.8 или более поздней версии.

Symantec AntiVirus (антивирусный клиент для 64+разрядных компьютеров):

- Windows XP 64-bit Edition Version 2003; Windows Server 2003 Enterprise/Datacenter 64-bit;
- не менее 32 Мб оперативной памяти;
- 70 Мб дискового пространства;
- Internet Explorer 4.01 или последующих версий;
- процессор Itanium 2.

Требования устаревших антивирусных клиентов

Symantec AntiVirus позволяет обеспечить антивирусную защиту на компьютерах Windows 95 с антивирусным клиентом Norton AntiVirus Corporate Edition 7.6.

Кроме этого:

- модуль Symantec AntiVirus требует дополнительно 6 Мб дискового пространства;
- модуль Symantec Client Firewall: 1 Мб дискового пространства;
- модуль Консоли изолятора: 35 Мб дискового пространства;
- модуль Alert Management System2: 24 Мб дискового пространства;
- средство развертывания сервера AV: 130 Мб дискового пространства;
- средство установки клиента NT: 2 Мб дискового пространства.

VirusScan

Вариант 1.

Workstation Requirements:

- Pentium or Celeron processor running a minimum of 166MHz;
- 32MB of RAM;
- minimum 38 MB free disk space;
- Windows NT 4.0 SP6 or greater;
- Windows XP Home and Professional SP1;
- Windows 2000 Professional SP3 or later;
- Microsoft Internet Explorer, version 5.0 or higher.

NOTE: VirusScan 4.5.1 supports Microsoft Windows 95/98/ME.

Server Requirements

- Pentium, Celeron, or Itanium processor running a minimum of 166 MHz;
- 32 MB of RAM;
- Minimum 38 MB free disk space;
- Windows NT 4.0 Server, SP 6 or greater; Windows NT 4.0 Enterprise Server, SP6 or greater;
- Windows 2000 Server SP1 or greater; Windows 2000 Advanced Server SP1 or greater;
- Windows Server 2003: Standard, Enterprise, or Web Edition;
- Microsoft Cluster Server (MSCS).

Other supported platforms: XP Tablet PC, Citrix MetaFrame 1.8 & XP Support; EMC Celerra File Server Support
Microsoft Internet Explorer, version 5.0 or higher.

Вариант 2.

VirusScan Enterprise is compatible with any of these Microsoft Windows platforms.

Workstation Server:

- Windows 2000 Professional, with SP4
- Windows 2000 Server, with SP4;
- Windows 2000 Advanced Server, with SP4
- Windows XP Home Edition, with SP1, SP2, or SP3;
- Windows XP Professional, with SP1, SP2, or SP3
- Windows 2000 DataCenter Server, with SP4;
- Windows Server 2003 Standard (32-bit and 64-bit), with SP1 or SP2;
- Windows XP Tablet PC Edition, with SP3;
- Windows Vista Home Basic;
- Windows Server 2003 Enterprise (32-bit and 64-bit), with SP1 or SP2;
- Windows Vista Home Premium;
- Windows Vista Business;
- Windows Server 2003 Web Edition (32-bit and 64-bit) SP1 and SP2;
- Windows Vista Enterprise;
- Windows Vista Ultimate;
- Windows Server 2003 R2 (32-bit and 64-bit) Standard, Enterprise, Web Edition;
- Windows Server 2003 R2 Datacenter Edition (32-bit and 64-bit);
- Windows Storage Server 2003;
- Windows Server 2008 (32-bit and 64-bit);
- Windows Server 2008 Datacenter (32-bit and 64-bit);
- Windows Server Core 2008 (32-bit and 64-bit);
- Browser — Microsoft Internet Explorer version 5.5 or later;
- Windows Installer — Microsoft Windows Installer (MSI) version 3.1 or later;
- Memory — 128 MB RAM (minimum) for a Pentium or Celeron processor running at 166 MHz and 256 MB RAM (minimum) for a Pentium II processor running at 350 MHz. For information on optimal operating system performance, review the Microsoft guidelines for RAM configuration;
- free disk space — 240 MB for a complete installation of all VirusScan Enterprise features and components, including a copy of the installation MSI file for repair ability.