



Сравнение функционала продуктов, предназначенных для защиты рабочих станций Windows



© ООО «Доктор Веб»,
2003–2010

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

Защити созданное

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	✗	✗	✗

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 сервера 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	✓			✗	✓		✗

Защита интернет-трафика							
Антивирусная проверка входящего и исходящего http-трафика	SplDer 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 фаервола
Ограничение доступа к ресурсам сети	✓	✗	✓	На уровне фаервола	✗		На уровне фаервола
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			

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	✓	✓				✓