Визитка

ВЯЧЕСЛАВ МЕДВЕДЕВ, *ведущий аналитик отдела развития ООО «Доктор Веб»*

В десятку!

Выбор нового функционала для любого популярного продукта напоминает ситуацию в басне Крылова: разработка настаивает на внедрении перспективных технологий, интересных программистам, отделы продаж заваливают пожеланиями от клиентов по типу «внедрите это, и мы купим на миллион», маркетинг напряженно вглядывается в будущее, пытаясь угадать, что будет модно у клиентов в следующем сезоне

Прогадать могут все – новые технологии будут непонятны клиентам, обещания купить останутся исключительно в переписке, на рынке возникнет новая мода, появления которой не предсказывал ни один аналитик. В системах безопасности ситуация осложняется необходимостью поддержки древних платформ и слабых конфигураций в связи с тем, что на них работают крупные клиенты.

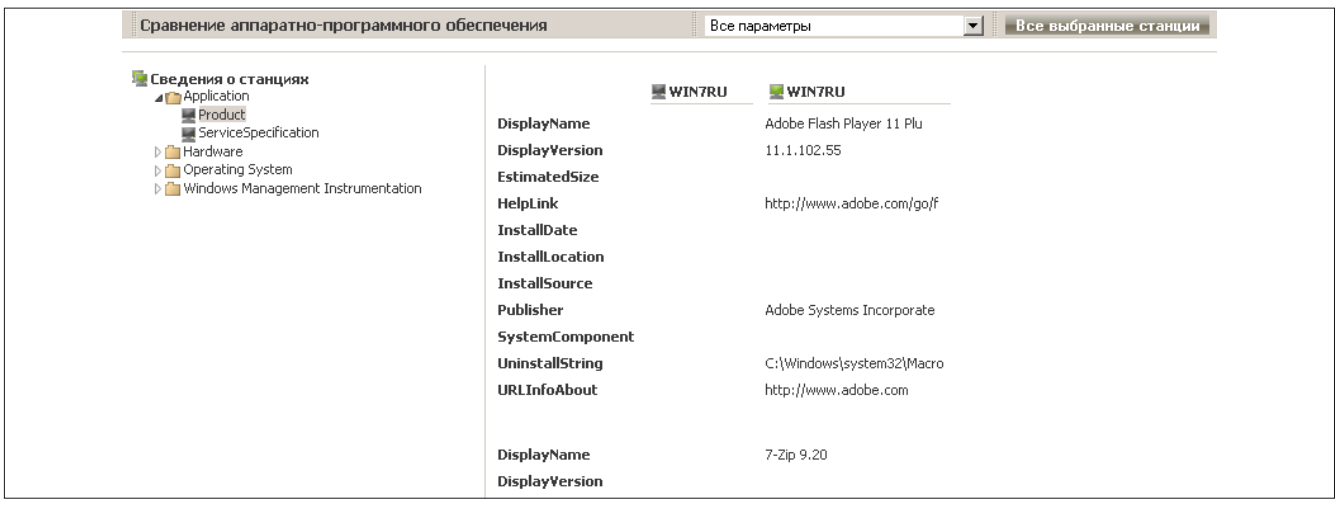
Не стал исключением и Dr.Web Enterprise Suite. Разработка новой версии велась несколько лет, и в результате только список нового функционала занимает более страницы, так что рассказать обо всех нововведениях в рамках выделенного размера статьи совершенно нереально. Поэтому остановимся только на ключевых особенностях и начнем, естественно, с возможностей по борьбе с вредоносными программами.

На уровне Dr.Web Агента для ОС Windows были реализованы:

- Подсистема непрерывного фонового сканирования и нейтрализации активных угроз.
- Превентивная защита, позволяющая предотвратить заражение операционной системы распространенными угрозами семейств Trojan.Encoder, Trojan.Inject и Trojan.Winlock. Наличие данного функционала, как и предыдущей подсистемы, крайне необходимо в связи с возможностью проникновения в защищаемую сеть вредоносных программ, протестированных на актуальных версиях антивирусных продуктов и потому не обнаруживаемых стандартными эвристическими механизмами.
- Новый алгоритм обнаружения угроз, которые были собраны неизвестными на текущий момент компоненту Dr.Web Virus-Finding Engine упаковщиками.
- Новая версия антируткит-модуля, предоставляющая возможность лучше обезвреживать угрозы, направленные на 64-разрядные операционные системы.

Необходимо отметить, что в ходе разработки антивирусных средств защиты всегда приходится учитывать печальный факт: с течением времени потребности средств защи-

Рисунок 1. Возможность просмотра и сравнения состава аппаратно-программного обеспечения на защищаемых станциях



ты в ресурсах системы только возрастают – в антивирусную лабораторию в месяц поступает на анализ семь-восемь миллионов файлов, что в итоге приводит к постоянному росту размера вирусных баз. Уменьшить потребность в той же оперативной памяти можно или разработкой новых технологий антивирусного ядра, обеспечивающих обнаружение модификаций уже известных семейств угроз, или переработкой компонентов средств защиты. В Dr.Web Enterprise Suite 10.0 в целях уменьшения потребления ресурсов на станциях с интенсивным файловым потоком был доработан файловый монитор.

Управление средствами безопасности для новой версии Dr.Web Enterprise Suite возможно как традиционным (рекомендованным приказами ФСТЭК России) способом – через веб-интерфейс, так и с помощью специального приложения для мобильных устройств – Мобильного центра управления, разработанного для применения на iPhone. Для устройств на основе Android управление эффективно осуществляется через браузер.

Согласно многочисленным пожеланиям увеличено количество способов, которыми можно провести развертывание системы. Добавлена установка с помощью полного дистрибутива, возможность синхронизации групп станций с Microsoft Active Directory. При наличии в сети нескольких серверов Active Directory установка агентов защиты может производиться с помощью возможностей службы распределенной файловой системы (DFS). В состав продукта вошли пакеты для установки антивирусных агентов на операционные системы Linux, FreeBSD, Android.

Добавлены возможности изменения первичной группы при автоматическом подтверждении доступа станций к Dr.Web Серверу и настройки правил автоматического распределения станций по пользовательским группам.

Стал возможен поиск станций, находящихся в разных доменах, и поиск станций в Active Directory и LDAP.

Внешний вид интерфейса Dr.Web Enterprise Suite остался практически неизменным, однако были существенно расширены возможности оперативного контроля за уровнем безопасности в антивирусной сети – введено автоматическое обновление выводимой информации, расширен раздел статистики и, самое главное, появилась возможность просмотра и сравнения состава аппаратно-программного обеспечения на защищаемых станциях (см. рис. 1).

Была улучшена система отчетов – в интерфейсе появилась возможность экспорта статистических отчетов антивирусной сети и их отправки по электронной почте через расписание антивирусного сервера. В число форматов, в которых возможен экспорт, был добавлен формат PDF.

Переработанная система оповещений администраторов, настраиваемая через Центр управления, теперь включает поддержку SNMP и дает возможность контроля за возникновением эпидемий.

Не осталась без изменений и система обновлений – была добавлена возможность обновления по защищенному каналу с использованием SSL-сертификатов, в состав решения вошла утилита автономной загрузки, что позволит упростить использование антивирусной защиты в сетях, не имеющих выхода в Интернет.

Также в связи с пожеланиями клиентов появилась возможность управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера (см. рис. 2).

Поскольку каналы доступа зачастую далеки от совершенства, механизмы получения обновлений были существенно переработаны.

В целях повышения надежности и отказоустойчивости реализована поддержка кластеров антивирусных серверов Dr.Web.

Стала более гибкой система назначения прав администраторов безопасности (см. рис. 3).

Опытные администраторы получили возможность работы с базой данных антивирусного сервера непосредственно из Центра управления – через SQL-консоль.

Существенным плюсом новой версии Dr.Web Enterprise Suite является то, что в одной локальной сети могут работать серверы разных версий. При этом серверы предыдущей, шестой, версии могут обмениваться статистикой с серверами новой. ADV

Рисунок 2. Возможность управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера

Рисунок 3. Система назначения прав администраторов безопасности