Как защитить данные от копирования на внешние носители

text:
Андрей Шуклин

Съемные носители представляют собой не только удобное хранилище для корпоративных данных, но и благоприятную среду для распространения вирусов. И даже если все сотрудники абсолютно лояльны (что бывает редко), риски информационной безопасности, связанные со съемными накопителями, сохраняют актуальность. Соответствующие средства защиты выпускают компании Lumension (Device Control), SecureIT (Zlock) и SmartLine Inc. (DeviceLock). Постараемся сравнить функционал этих продуктов и дать рекомендации по их использованию.

Ключевые особенности решений

Начнем с Lumension Device Control (LDC). Будучи частью платформы Lumension Endpoint Management and Security Suite, эта система включает в себя различные модули для контроля доступа к внешним устройствам и сетевым интерфейсам (собственно Device Control), контроля приложений (Aplication Control), передаваемого контента, распространения патчей и обновлений (Patch and Remediation). С ее помощью можно создать комплексную систему информационной безопасности, обеспечив защиту чувствительных данных от утечки через любые каналы связи и поддержку всех программных компонентов рабочих станций в актуальном состоянии.

Основное назначение системы Zlock — предотвращение утечек конфиденциальной информации через периферийные устройства. Решение разграничивает доступ к накопителям и принтерам, анализирует содержимое файлов, распечатываемых и записываемых на устройства, блокирует действия пользователей в случае выявления нарушений политик безопасности, а также дает возможность гибко настраивать права доступа пользователей и групп пользователей к любым устройствам. Анализируются как внешние порты (USB, LPT, COM, IrDA, PCMCIA, IEEE 1394), так и внутренние устройства (сетевые карты, модемы, Bluetooth, Wi-Fi, CD/DVD), контролируется доступ к локальным и сетевым принтерам.

Средство защиты от утечек информации (DLP) — система DeviceLock — позволяет контролировать и протоколировать доступ пользователей к устройствам, портам ввода-вывода и сетевым протоколам. А кроме того, контролировать буфер обмена Windows, простые и защищенные сессии электронной почты, HTTP- и HTTPS-сессии, веб-почту и социальные сети, службы мгновенных сообщений, файловый обмен.

Сравниваем функционал

Базовый функционал перечисленных средств позволяет повысить безопасность корпоративной сети и предотвратить возможные утечки данных через подключаемые к ПК устройства. Любое из трех решений можно централизованно установить на рабочие станции, привязать к общей службе каталогов, такой как Active Directory, и настраивать через центральную консоль. Однако на практике применение каждой системы имеет свои особенности, поэтому выбирать их необходимо с учетом требований к уровню защиты, архитектуры корпоративной сети и ряда других параметров.

Так, решение LDC позволяет полностью контролировать копирование файлов на съемные носители, не блокируя возможность использования USB-портов, например, для подключения принтера, сканера и других периферийных устройств (имеющиеся в организациях системы полной блокировки USB-портов серьезно ограничивают возможности сотрудников). LDC обеспечивает доступ в определенном промежутке времени, например на 15 минут после поступления запроса администратору. Можно настроить также постоянный график доступа для определенных пользователей или устройств — система отличает их по серийному номеру.

Реализованная по умолчанию в LDC и Zlock возможность фильтрации устройств по белому списку (когда на подключение различных интерфейсов выдается персональное разрешение для определенных пользователей) вызывает в DeviceLock затруднения: настройка белого списка происходит лишь с использованием встроенных категорий, а разрешенные устройства оказываются доступными для всех пользователей, а не выборочно.

Сильная сторона Zlock — возможность контентной фильтрации документов, передаваемых через сетевые интерфейсы, записываемой на носители информации или распечатываемой на принтере. Благодаря этому администратор может очень точно прописать политики фильтрации содержимого, основываясь на особенностях различных конфиденциальных документов. Впрочем, очевидно, что такой функцией воспользуются далеко не все заказчики, так как без тщательной настройки она будет давать лишь ложные срабатывания. Например, в линейке Lumension функция контентной фильтрации реализована в отдельной системе, которая может применяться дополнительно в рамках LEMSS. В решении DeviceLock также возможно применение контентной фильтрации при установке дополнительного компонента — ContentLock.

Если в вашей компании используются тонкие клиенты, наиболее подходящим вариантом станет LDC, так как только в этой системе реализована возможность контроля соответствующих устройств. DeviceLock и Zlock могут обеспечить безопасность данных только на традиционных ПК. Кроме того, LDC не использует специальных протоколов для связи между сервером и клиентом — весь служебный трафик передается только по TCP/IP, позволяя централизованно применять систему в сложных корпоративных сетях, разделенных межсетевыми экранами, виртуальными туннелями и состоящих из различных сегментов.

Что касается теневого копирования — сохранения копий данных на съемные носители для последующего анализа, то во всех трех системах данный функционал реализован по-разному. Zlock делает это в собственной базе данных на клиентской машине, LDC сохраняет на отдельном диске по выбору администратора, а DeviceLock позволяет администратору выделить дисковое пространство специально для теневых копий. Правда, в случае с DeviceLock возможности теневого копирования доступны только для предопределенных классов устройств, уже имеющихся в системе (отсутствует возможность выборочного назначения устройств для теневых копий). В Zlock же есть интересная возможность теневого копирования данных, отправляемых на печать, что позволяет контролировать обращения к принтерам отдельных пользователей, например тех, кто имеет доступ к чувствительной информации.

LDC и Zlock обладают широкими возможностями в плане создания групп пользователей и устройств, что позволит администратору применять общие политики безопасности для большого количества рабочих станций. В этих системах устройства разделены на множество классов, обеспечивая возможность более гибко управлять доступом к периферии. В DeviceLock, напротив, все USB-устройства относятся к одному классу, а это влечет к необходимость выдачи персонального разрешения на использование каждого сканера или сетевого интерфейса.

Интересную возможность предусмотрели разработчики LDC, позволив создавать условные разрешения: например, открывать доступ на запись только определенному пользователю, только в определенное время, только для ограниченного объема данных и только для определенных типов файлов. Можно настраивать политики включения/отключения устройств с учетом сразу множества параметров.

Наконец, еще одна сильная сторона LDC — интеграция клиентской части на уровне ядра — предотвращает возможность удаления или отключения сервиса даже на правах локального администратора и на компьютере, не подключенном в данный момент к корпоративной сети. В Zlock данная функция реализована на уровне сервиса, который при повреждении или удалении драйвера блокирует доступ к ПК любым пользователям, кроме администратора.

Заключение

В результате сравнительного тестирования наиболее сбалансированным решением показала себя система Lumension Device Control. Устойчивое к воздействиям ядро клиентской части делает данный продукт надежным, а консоль настройки групповых политик, доступная в базовой версии, позволяет легко настроить его использование даже в распределенной сети, в том числе содержащей тонкие клиенты и удаленные рабочие места, находящиеся за брандмауэром. По совокупности параметров мы награждаем Lumension Device Control медалью «Выбор эксперта». ◑●●

Сравнительные характеристики решений

	DeviceLock	Lumension Device Control	Zlock
Централизованное управление	да	да	да
Поддержка Active Directory	да	да	да
Создание групп устройств для управления	нет	да	да
Создание групп компьютеров для управления	нет	да	нет
Защита по принципу белого списка	нет	да	да
Контентная фильтрация	нет	нет	да
Шифрование данных	да	да	да
Централизованный журнал и архив	да	да	да
Защита при отсутствии подключения к серверу	да	да	да
Драйвер на уровне ОС клиента	нет	да	нет
Теневое копирование	да	да	да
Выбор дискового пространства для теневых копий	да	да	нет
Блокировка IDE/ATA	нет	да	да
Блокировка SCSI	нет	да	нет
Блокировка беспроводных портов	да	да	да
Зависимые политики запрета записи	нет	да	нет
Связь между сервером и клиентом по IP	нет	да	нет
Автоматический контроль целостности файлов	нет	да	да
Возможность работы на тонких клиентах	нет	да	нет