Не дайте информации
утечь сквозь пальцы ...

DeviceLock®

Противодействие утечкам конфиденциальной информации и персональных данных

Тарашкевич Артём

Компания БАКОТЕК

WIKILEAKS…

Факторы инсайдерских угроз

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

- Непреднамеренные утечки: ошибки и халатность
- Преднамеренные утечки: превышение полномочий, чрезмерное усердие («доработка на дому»)
- Направленные утечки: злоумышленники, шпионаж

ТЕХНОЛОГИЧЕСКИЙ ФАКТОР

- Распространение скоростных беспроводных сетей
- Рост размеров памяти носителей при снижении цены, габаритов и простоте использования (pnp)
- Проникновение вирусов с личных съемных носителей сотрудников

Каналы утечки данных

ВО ВРЕМЯ ЭКОНОМИЧЕСКОГО КРИЗИСА, СОГЛАСНО ИССЛЕДОВАНИЯМ PONEMON INSTITUTE И SYMANTEC, БОЛЕЕ 60% УВОЛЬНЯЕМЫХ СОТРУДНИКОВ «СОХРАНЯЮТ ЗА СОБОЙ» КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ СВОИХ КОМПАНИЙ

Сетевые каналы

Локальные каналы

Традиционные решения информационной безопасности

ДЛЯ ПОЛНОЦЕННОГО РЕШЕНИЯ ПРОБЛЕМЫ ИНСАЙДЕРСКИХ УТЕЧЕК ДАННЫХ НЕОБХОДИМО ИСПОЛЬЗОВАНИЕ СПЕЦИАЛИЗИРОВАННОГО ПРОДУКТА

ФОКУС НА ВНЕШНИХ УГРОЗАХ

- Защита от хакеров и внешних вторжений (межсетевые экраны, ips)
- Антивирусы, анти-спам, контентные фильтры почты, др.
- Системы авторизации, токены, vpn для доступа пользователей к важной информации извне
- Контролируемые почтовые серверы, средства фильтрации контента
- Запрет im и альтернативных почтовых ящиков

НЕТ КОНТРОЛЯ ЛОКАЛЬНЫХ КАНАЛОВ

- Традиционные сетевые СЗИ – бесполезны против устройств хранения данных
- Тотальный запрет КПК, удаление USB, ограничение печати – контрпродуктивны для бизнеса и нереальны в исполнении
- Встроенные в Vista и Windows 7 технологии малоэффективны

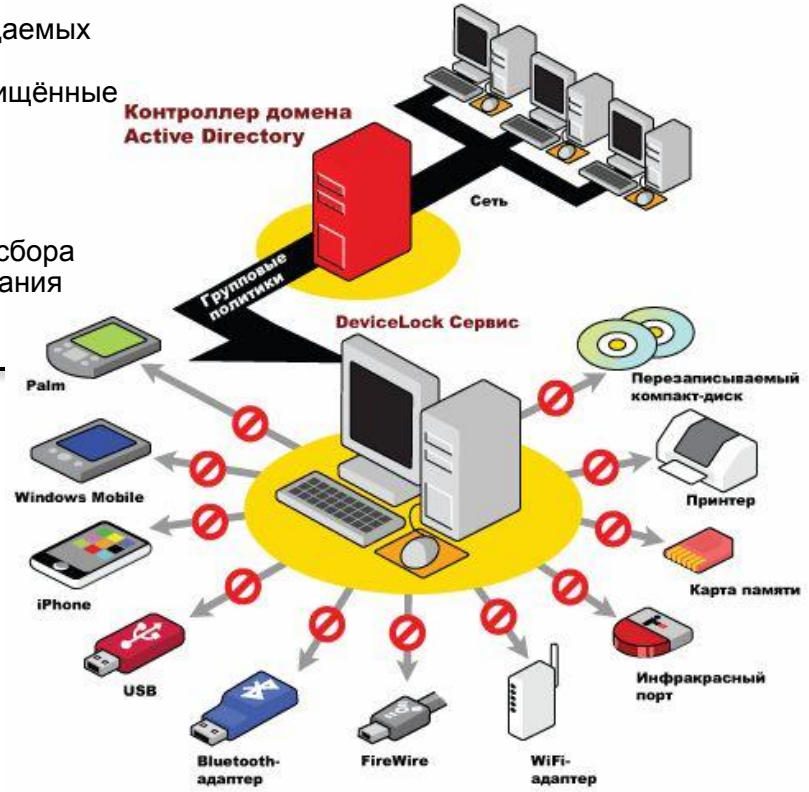
Ключевые требования

- Настраиваемый контроль всего спектра устройств (внешних и внутренних) и портов; принцип «достаточности привилегий»
- «Невидимость» для пользователей – пока не нарушены политики доступа
- Масштабируемость от СМБ до больших корпоративных сред
- Протоколирование (аудит) действий пользователей и администраторов для дальнейшего анализа исследования
- Интегрируемость с другими решениями ИБ
- Лёгкость развертывания и эксплуатации – централизация и прозрачность для администраторов ИБ
- Устойчивое противодействие попыткам неавторизованного изменения политик безопасности и/или отключения
- Доступная цена, качественная поддержка

DeviceLock

АРХИТЕКТУРА КОМПЛЕКСА

- Исполнительные агенты на защищаемых ПК, незаметные для пользователей и полностью защищённые от деструктивных воздействий
- Платформа централизованного управления с несколькими вариантами консолей и сервером сбора данных аудита и теневого копирования



ПРОГРАММНЫЙ КОМПЛЕКС КОНТРОЛЯ

- Контроль доступа к локальным портам и интерфейсам пк и серверов
- Предотвращение утечек данных и проникновения вредоносного ПО

ГРАНУЛИРОВАННОСТЬ КОНТРОЛЯ

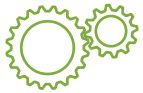
- Гранулированный контроль и аудит всех типов каналов локальной утечки данных, в особенности Local Sync (мобильные устройства)
- Интеграция с внешними средствами шифрования съёмных носителей без объединения кода

УНИКАЛЬНЫЕ МАСШТАБИРУЕМОСТЬ, ЭКОНОМИЧНОСТЬ И НАДЁЖНОСТЬ

- Полноценная интеграция управления жизненным циклом агентов в платформу microsoft Active Directory
- Реальные проекты – до 70 тыс. ПК, более 4 млн. копий по всему миру

Операционные платформы

DEVICELOCK SERVICE



Агент DeviceLock, устанавливаемый на каждом клиентском компьютере. Запускается автоматически, обеспечивает защиту устройств на уровне ядра ос, оставаясь невидимым для локальных пользователей

Windows NT/2000/XP/2003/Vista/2008, Windows 7 (32/64-bit)

DEVICELOCK ENTERPRISE SERVER

Используется для сбора и централизованного хранения данных теневого копирования, а также централизованного мониторинга агентов и применяемых политик безопасности.

Microsoft SQL, MSDE, ODBC-совместимые БД

DEVICELOCK MANAGEMENT CONSOLE

Оснастка для MMC.
Используется для управления настройками DeviceLock Service, Devicelock Enterprise Server и просмотра журналов аудита и данных теневого копирования

DEVICELOCK ENTERPRISE MANAGER

Используется для одновременного управления множеством компьютеров.
Использует многопоточный механизм выполнения действий, что ускоряет их выполнение.
Рекомендуется для больших сетей, не использующих MS Active Directory. MS AD, Novell eDirectory, LDAP

DEVICELOCK GROUP POLICY MANAGER

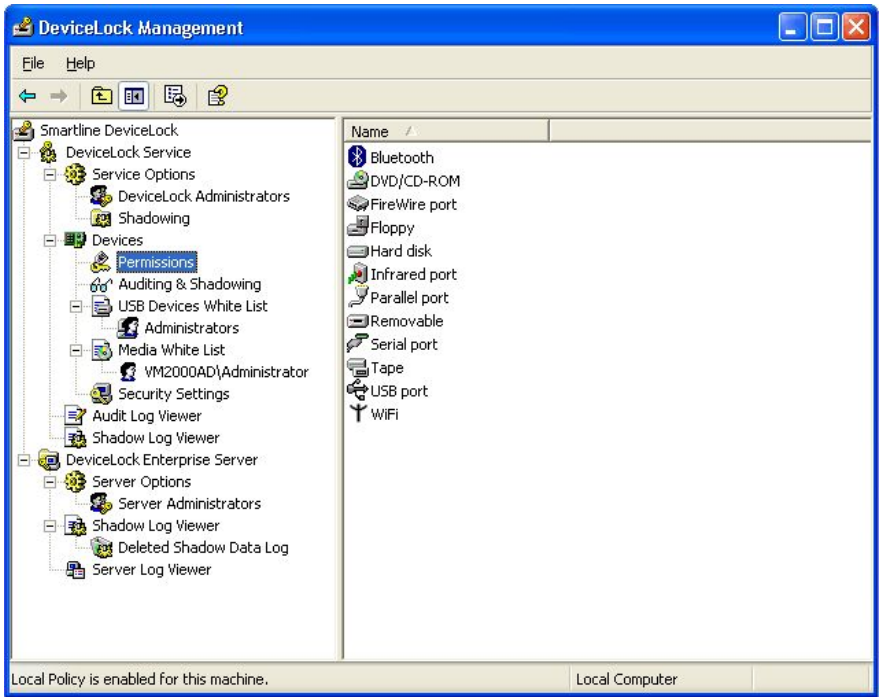
Используется для управления настройками DeviceLock через групповые политики контроллера домена Active Directory.
Интегрируется в редактор групповых политик (GPO Editor). MS AD (полностью)

Гранулированность контроля (1/2)

КОНТРОЛИРУЕМЫЕ ОБЪЕКТЫ
- Пользователи, их локальные и доменные группы
- Компьютеры и групповые объекты в active directory

ЛЮБЫЕ ТИПЫ СТАНДАРТНЫХ ПОРТОВ/ИНТЕРФЕЙСОВ И УСТРОЙСТВ

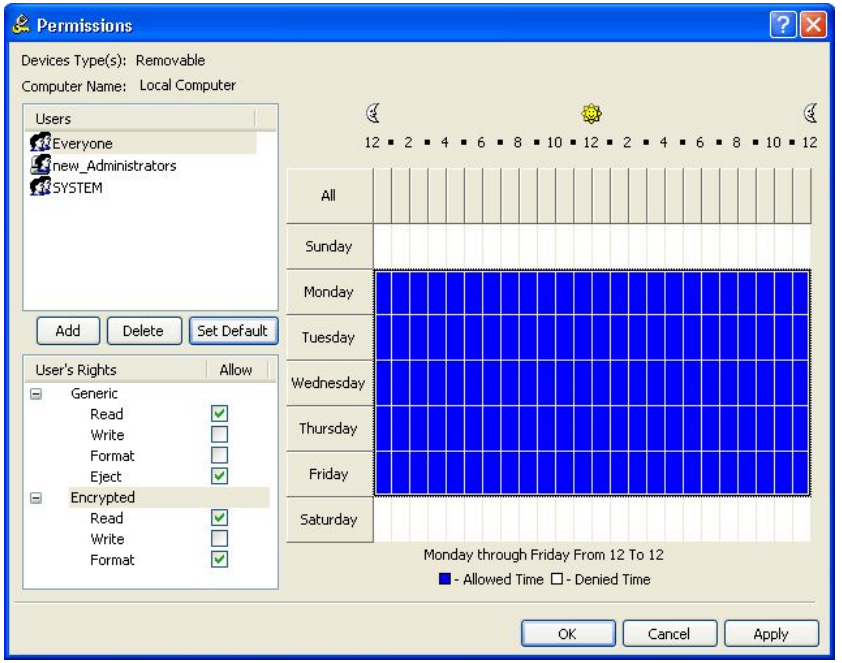
USB,
FireWire,
LPT,
COM,
Irda,
Removable,
HDD,
Floppy,
DVD/CD-ROM,
Tape,
Modem,
Bluetooth,
Wi-Fi,
мобильные устройства,...



Гранулированность контроля (2/2)

ОПЕРАЦИИ
Чтение, запись, форматирование, извлечение устройства

ГИБКИЙ ГРАФИК КОНТРОЛЯ ДОСТУПА И АУДИТА
Время и дни недели

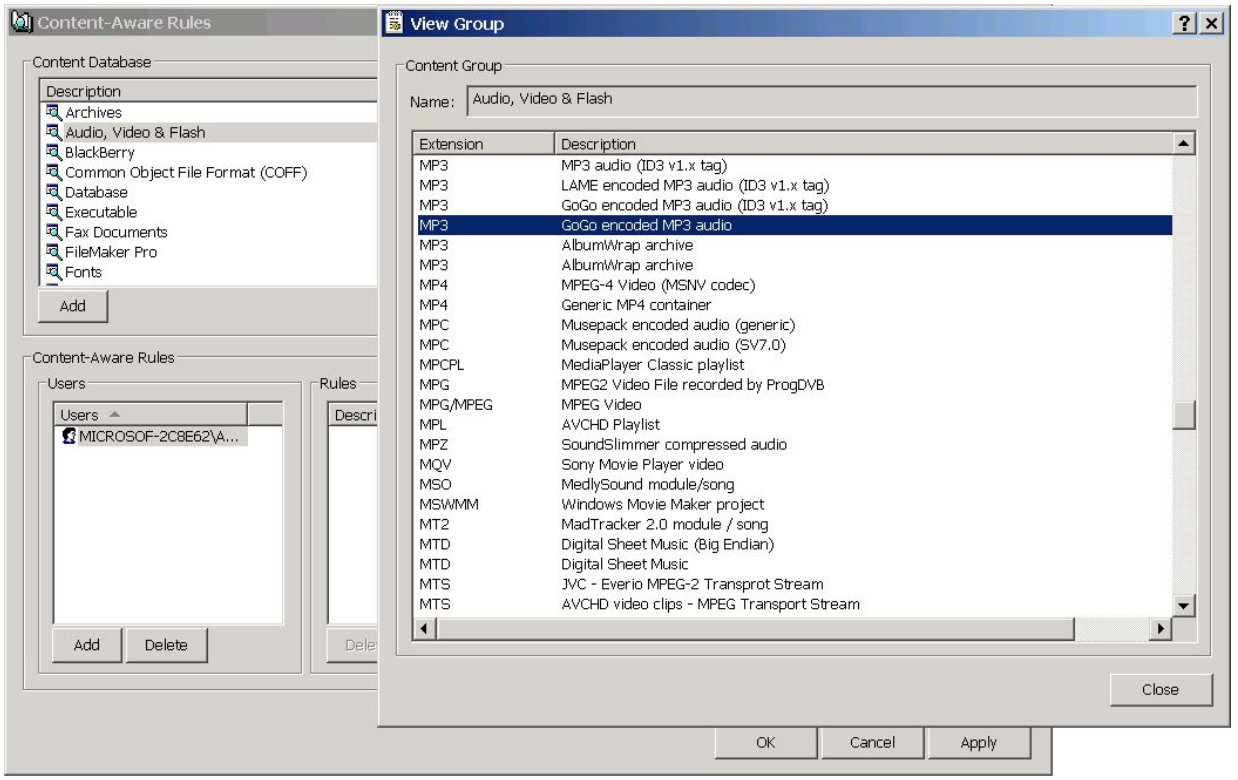


«БЕЛЫЕ СПИСКИ»
•Белый список USB-УСТРОЙСТВ: по производителю, модели, серийному номеру, по пользователям/группам пользователей
•«Временный» белый список (предоставление доступа к устройству без внесения его в белый список носителей (CD/DVD), по пользователям/группам пользователей

Фильтрация по типам файлов

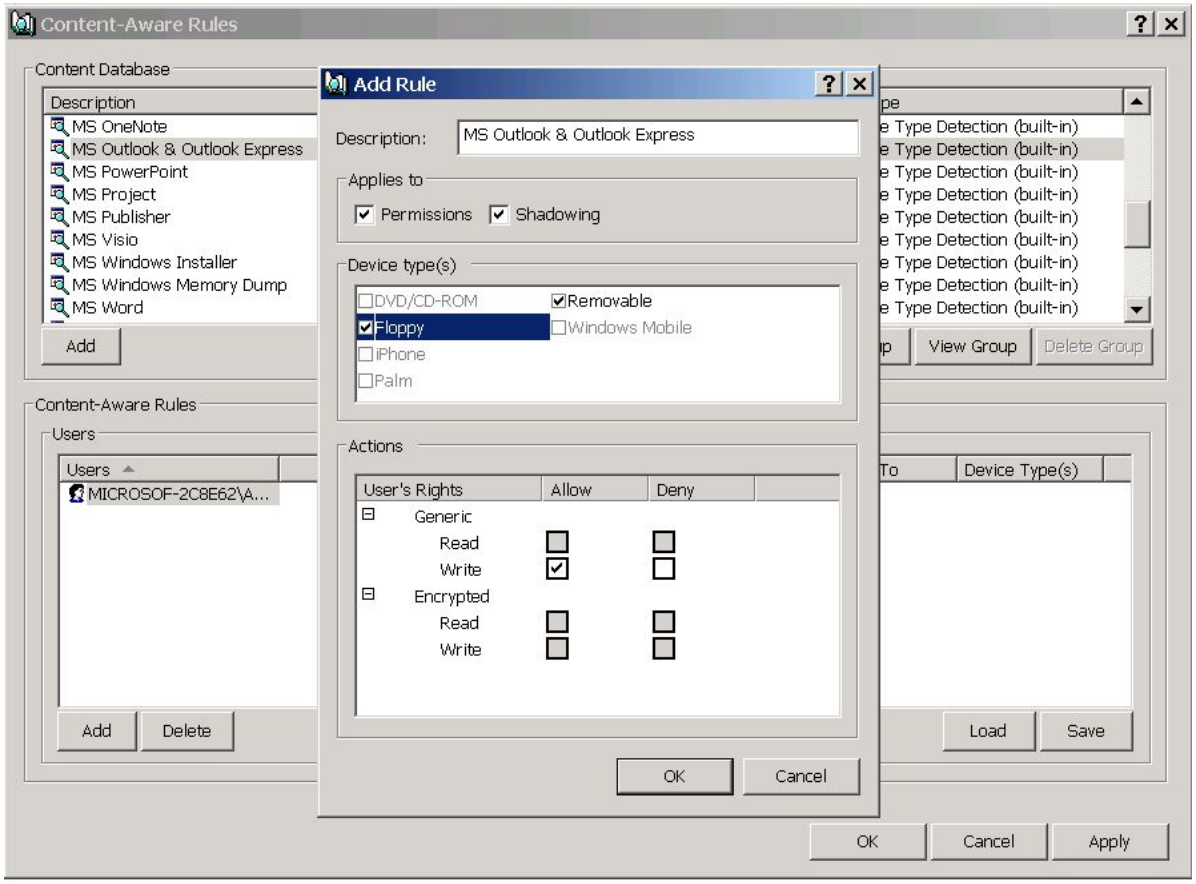
БИНАРНО-СИГНАТУРНЫЙ МЕТОД ДЕТЕКТИРОВАНИЯ ТИПОВ ФАЙЛОВ НА ОСНОВЕ ПОЛНОГО АНАЛИЗА СОДЕРЖИМОГО ФАЙЛА

- Поддержка около 4 000 форматов
- Возможность добавления поддержки новых форматов



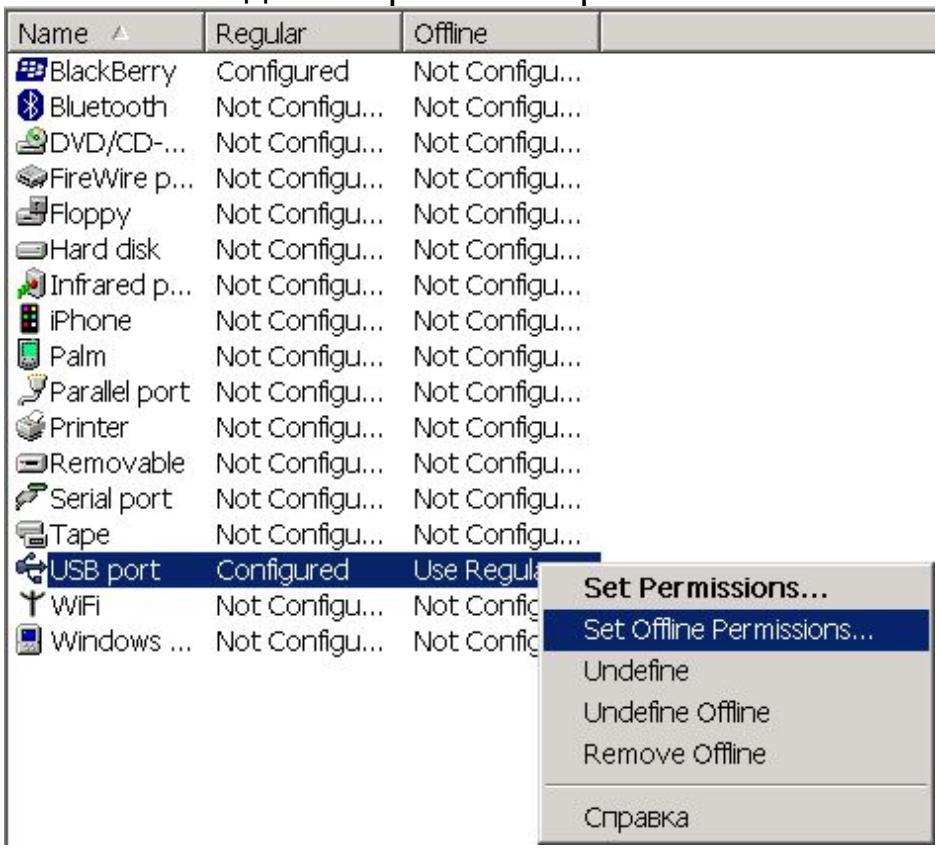
Политики протоколирования и теневого копирования

ИЗБИРАТЕЛЬНЫЕ ПОЛИТИКИ ПРОТОКОЛИРОВАНИЯ И ТЕНЕВОГО КОПИРОВАНИЯ С ТОЧНОСТЬЮ ДО ТИПОВ ФАЙЛОВ



Политики Offline\Online

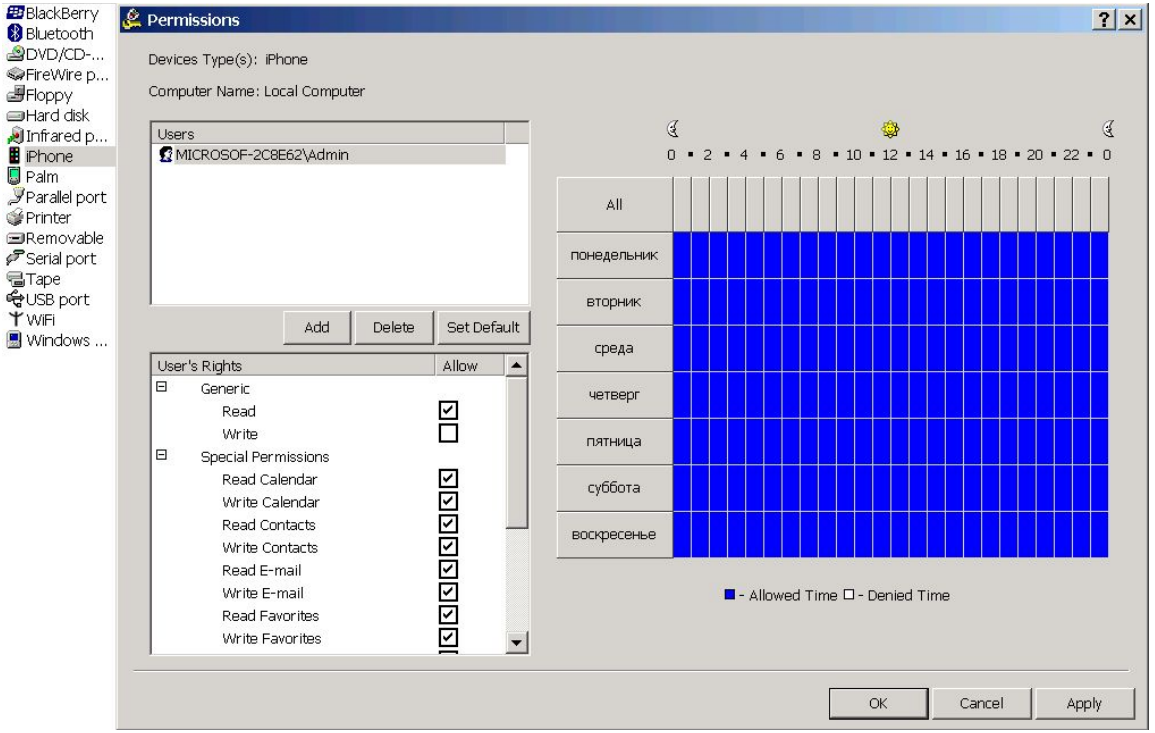
ЗАДАНИЕ РАЗНЫХ ПОЛИТИК ДЛЯ КОМПЬЮТЕРОВ ONLINE/OFFLINE
С автоматическим детектированием режимов



Расширенный контроль мобильных устройств (1/2)

- Контроль локальной синхронизации данных между компьютерами пользователей и их персональными мобильными устройствами
на базе ОС Windows Mobile, Palm OS (КПК, смартфоны), iPhone/iPod, Blackberry

- Гранулированность контроля – по типам протокольных объектов
  - Файлы,
  - графические объекты,
  - календарь,
  - e-mail,
  - задачи,
  - заметки,…
  - Управление удаленными инсталляцией и исполнением приложений



Расширенный контроль мобильных устройств (2/2)

- Детектирование мобильных устройств на любых интерфейсах:
  USB, COM, IRDA, Bluetooth

- Детальное централизованное протоколирование и теневое копирование данных, переданных по каналам локальной синхронизации

- Централизованное администрирование и управление доступом к мобильным устройствам на основе политик

Контроль канала печати (1/3)

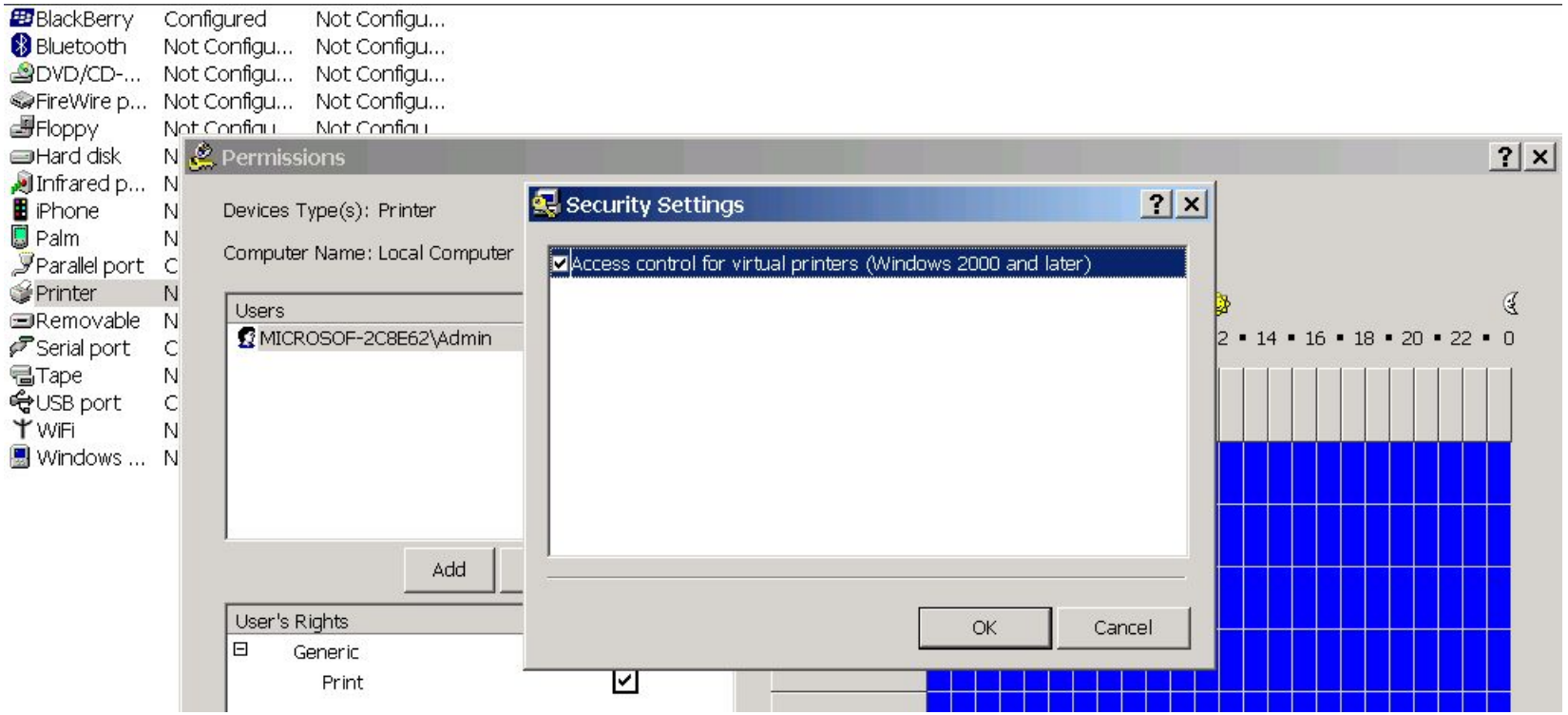
Гранулированный централизованный контроль доступа пользователей к любым локальным и сетевым принтерам

Параметры контроля
- Кто – пользователи и их группы, объекты из Active Directory
- Когда – недельный график с точностью до дня и часа
- Какой принтер –
  - Локальный / сетевой / виртуальный
  - Интерфейсы USB, LPT, Bluetooth, WiFi
  - USB: с точностью до уникального принтера (по серийному номеру)

Централизованное протоколирование и теневое копирование данных в канале печати
- Просмотр сохраненных документов в графическом виде для форматов спулера печати: PS, PCL 5/6, HP-GL/2, GDI, EMF, SPLC
- Печать документов, сохраненные в бд теневого копирования
- Экспорт в форматах BMP, GIF, JPEG, PNG, EMF, TIFF

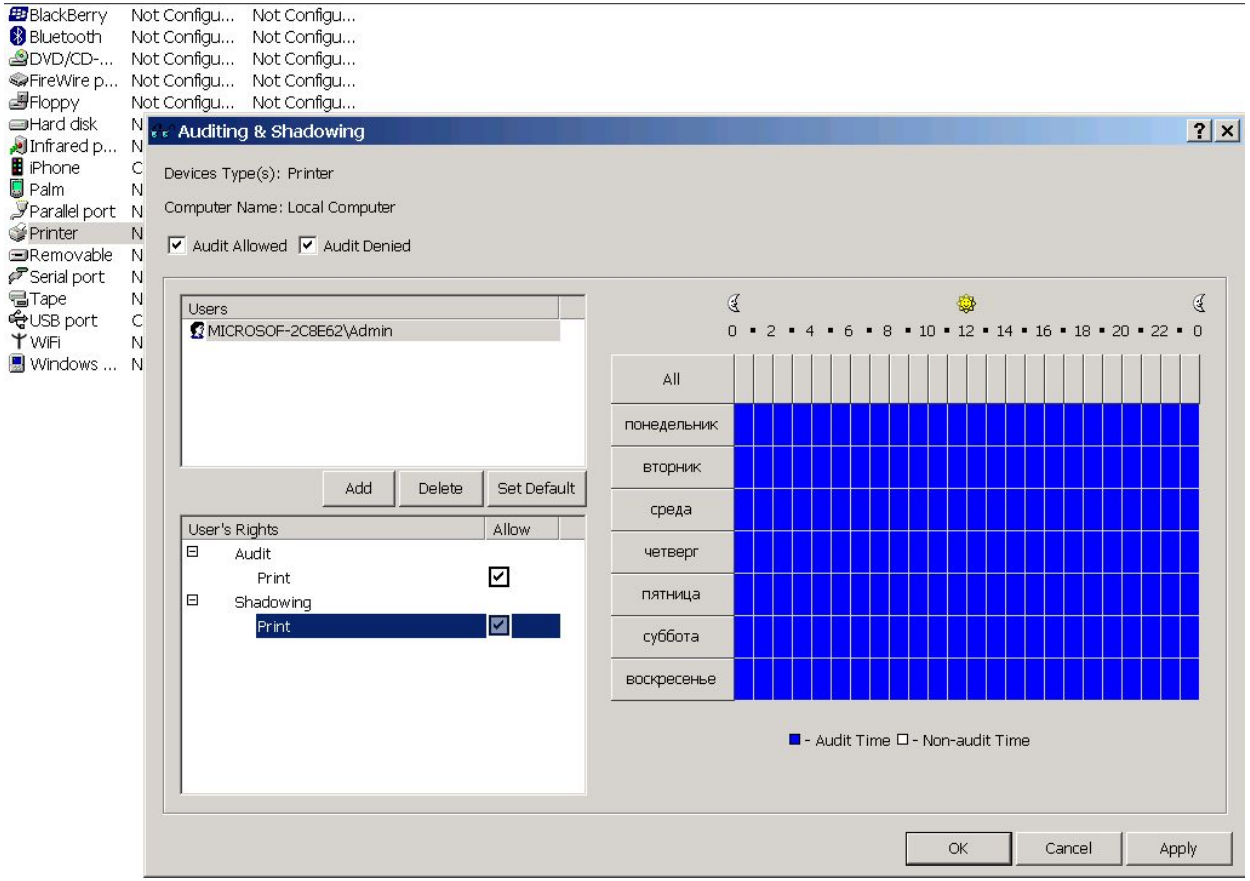
Контроль канала печати (2/3)

Контроль устройств



Контроль канала печати (3/3)

Аудит и теневое копирование операций принтера



ПОДДЕРЖКА ВНЕШНЕГО ШИФРОВАНИЯ ДАННЫХ

DeviceLock поддерживает :

- PGP Whole Disk Encryption
- TrueCrypt*
- SafeDisk 4
- Lexar SAFE PSD

ИНТЕГРИРОВАННОЕ РЕШЕНИЕ ПО КОНТРОЛЮ ШИФРОВАНИЯ СЪЁМНЫХ УСТРОЙСТВ ПАМЯТИ

- Предотвращает несанкционированный экспорт данных на съёмные устройства памяти в нешифрованном виде
- При этом не запрещает сохранять их зашифрованными с помощью SafeDisk на разрешённых к применению внешних устройствах для использования в служебных целях

Управление и администрирование

ПОЛНАЯ ИНТЕГРАЦИЯ В СРЕДУ MICROSOFT ACTIVE DIRECTORY
- Инсталляция, управление и администрирование из домена AD через групповые политики без выделенного сервера управления
- Автоматическая установка на новые компьютеры, в т.ч. преконфигурируемая
- Использование стандартной оснастки Group Policy Editor
- Поддержка RSoP

ПОЛНОФУНКЦИОНАЛЬНАЯ СОБСТВЕННАЯ ПЛАТФОРМА УПРАВЛЕНИЯ, НЕ ТРЕБУЮЩАЯ ВЫДЕЛЕННЫХ СЕРВЕРОВ УПРАВЛЕНИЯ И РАСШИРЕНИЯ ИНФРАСТРУКТУРЫ КОМПАНИИ

ОНЛАЙН-МОНИТОРИНГ СОСТОЯНИЯ И ВОССТАНОВЛЕНИЕ ПОЛИТИК АГЕНТОВ

ИНСТАЛЛЯЦИЯ АГЕНТОВ
- Локальная интерактивная или преконфигурируемая
- Централизованная без участия пользователей

КОМПРЕССИЯ ДАННЫХ И УПРАВЛЕНИЕ ПРИОРИТЕТНОСТЬЮ ТРАФИКА ПРИ АВТОМАТИЧЕСКОМ СБОРЕ ДАННЫХ АУДИТА И ТЕНЕВОГО КОПИРОВАНИЯ С АГЕНТОВ В ЦЕНТРАЛЬНУЮ БД

DeviceLock Content Security Server

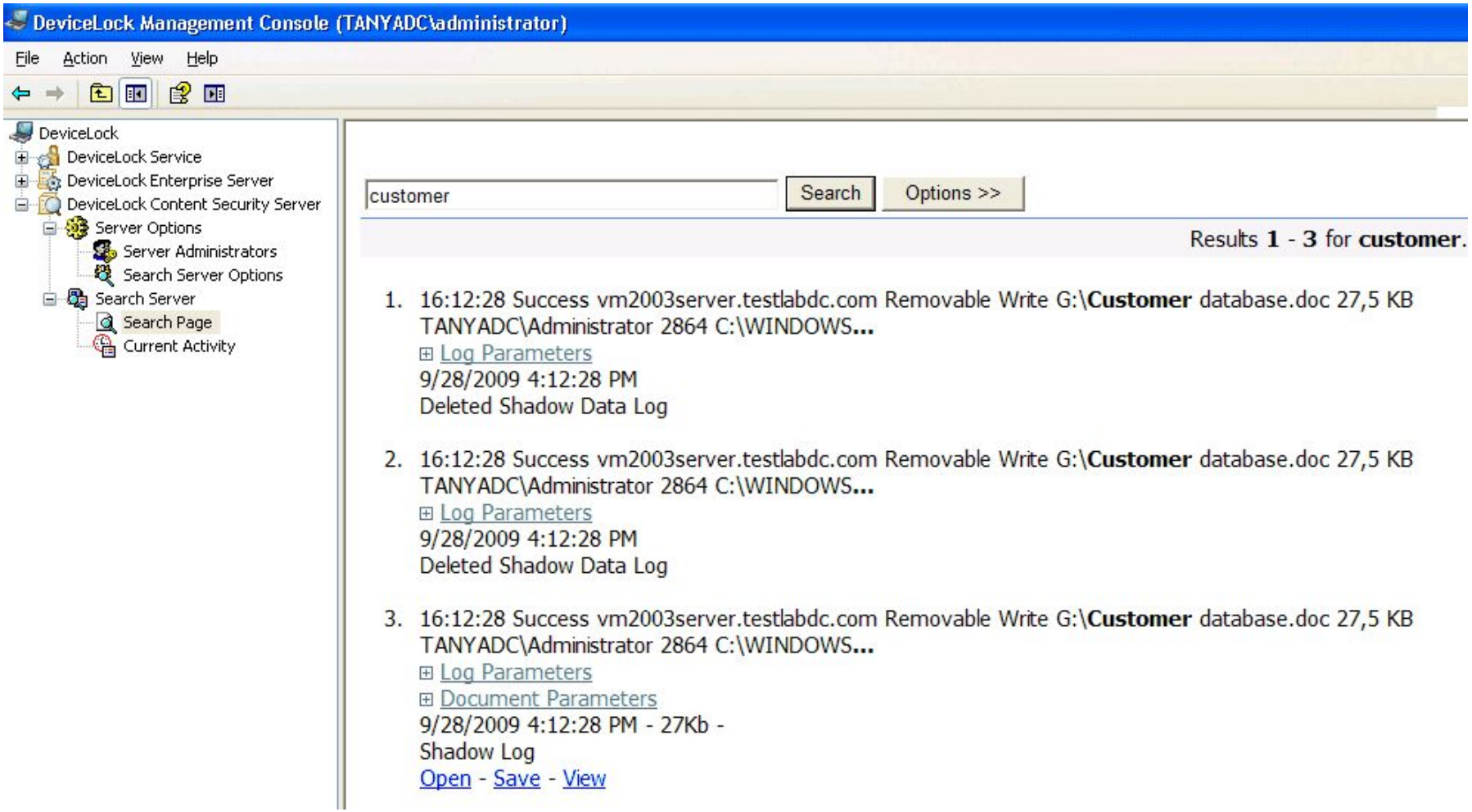
DEVICELOCK CONTENT SECURITY SERVER
Отдельный компонент, являющийся оболочкой для дополнительных модулей DeviceLock, направленных на работу с контентом

DEVICELOCK SEARCH SERVER (ПОИСКОВЫЙ СЕРВЕР)
Позволяет осуществлять полнотекстовый поиск по базам данных теневого копирования (внутри сохраненных файлов) и журналам аудита, хранящимся в DeviceLock Enterprise Server

DEVICELOCK SEARCH SERVER МОЖЕТ АВТОМАТИЧЕСКИ РАСПОЗНАВАТЬ, ИНДЕКСИРОВАТЬ, НАХОДИТЬ И ОТОБРАЖАТЬ ДОКУМЕНТЫ МНОЖЕСТВА ФОРМАТОВ
Adobe Acrobat (PDF), Ami Pro, архивы (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works, OpenOffice (документы, таблицы и презентации), Quattro Pro, WordPerfect, Wordstar и многих других

DLSS лицензируется отдельно от DeviceLock, по количеству индексируемых записей в журналах

DeviceLock Search Server



Планы: DeviceLock 7.0

- ContentLock поддерживает контентную фильтрацию файлов, копируемых на съемные устройства хранения любых типов

- NetworkLock контроль содержимого объектов данных, передаваемых с компьютера через каналы сетевых коммуникаций, включая приложения электронной почты, интерактивные web-сервисы, социальные сети, форумы и конференции, наиболее популярные службы мгновенных сообщений (Instant Messengers), файловые обмены по протоколу FTP, а также Telnet-сессии

Поддержка

- Система Online HelpDesk (www.devicelock.com/ru/support) – сайт, e-mail
- Форум, «Часто задаваемые вопросы», Документация и справочные материалы
- Онлайн-семинар
- Для расширенной технической поддержки:
  - телефонная линия поддержки
  - IM-линия поддержки
  - выезд специалиста на место эксплуатации
  - персональный менеджер поддержки

DeviceLock. – 13 лет на рынке!

- Смарт Лайн Инк – российская компания, основанная в 1996 году, специализируется на разработке программного обеспечения, контролирующего доступ сотрудников к портам и мобильным устройствам
- За 13 лет клиентами «Смарт Лайн Инк» стали более 60 тысяч компаний в 90 странах мира
- Штат компании – 50+ человек (20+ разработчиков)
- Штаб-квартира и подразделение разработки – Москва
- Торговые офисы в США, Великобритании, Германии, Италии
- Общий объем инсталляций DeviceLock превышает 4 миллиона экземпляров (самая большая – 68 тыс.)

Кому необходим DeviceLock?

- Государственные организации, работающие с конфиденциальной информацией
- Компании от Small до Enterprise нуждающиеся в контроле доступа к устройствам для приема, передачи или обработки данных.
- Организации работающие на высоко конкурентном рынке

Лицензирование и политика обновлений

Цены для **конечных** пользователей (USD)	
1-4 Single-лицензий	53
5-10 Single-лицензий	49
11-50 Single-лицензий	45
51-100 Single-лицензий	37
101-1000 Single-лицензий	29
1001-2000 Single-лицензий	25
2001-5000 Single-лицензий	21
от 5001 Single-лицензии	17

- Обновления и новые версии DL : бесплатно в течение 1 года с момента приобретения
- При покупке обновлений в течение 13 месяцев с момента начальной покупки: 30% стоимости лицензий по прайс листу
- При покупке обновлений по истечении 13 месяцев с момента начальной покупки: 70% стоимости лицензий по прайс листу.

Клиенты


БАНК РОССИИ
ПЕРЕКРЕСТОК
КапиталЪ
Страхование
РОССИЙСКАЯ ГОСУДАРСТВЕННАЯ БИБЛИОТЕКА
АТОМЭНЕРГОПРОЕКТ
САНКТ-ПЕТЕРБУРГ
ГУТА СТРАХОВАНИЕ
ВТБ24
МДМ Банк
U.S. AIR FORCE
DEPARTMENT OF THE NAVY
UNITED STATES OF AMERICA
METROPOLITAN POLICE
LAMBORGHINI
Ferrari
BARCLAYS
HSBC
The world's local bank
Microsoft UK
CHASE
ENGINEERING
AEROTEC
BNP PARIBAS
Triodos Bank
Make your money make a difference

DeviceLock®

СПАСИБО ЗА ИНТЕРЕС К DEVICELOCK!

БАКОТЕК
info@bakotech.ua
www.bakotech.ua

(044) 273 33 33

Artem.tarashkevych@bakotech.ua
Артем Тарашкевич

www.devicelock.com