Lumension™
IT Secured. Success Optimized.

Lumension Device Control (LDC)

headtechnology
it-security

Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance

www.lumension.com

Lumension
IT Secured. Success Optimized.

WWW.DATALOSSDB.ORG

1000 файлов с именами, историей болезни, даты лечения – потеряны на персональном ПК

Хакеры взломали доступ к беспроводной сети. Украдена информация о 50 картах клиентов

Украдено 1600 записей с номерами и именами счетов социального страхования

краден ноутбук с информацией о 75.000 счетах клиентов

Украден винчестер с номерами карт социального страхования

Украден или потерян ноутбук содержащий медицинские данные 3500 пациентов

Количество устройств

Сколько?

более 4,800,000,000 шт в 2010 г.

- Миллиарды проданных устройств
  - Ipods, Memory sticks etc
- Растущая мощность устройств
  - 32GB SD cards
- Множество разных форм и типов
  - В виде ручек, игрушек, ножиков, часов
- Снижение стоимости
  - 2GB USB стоит менее $11

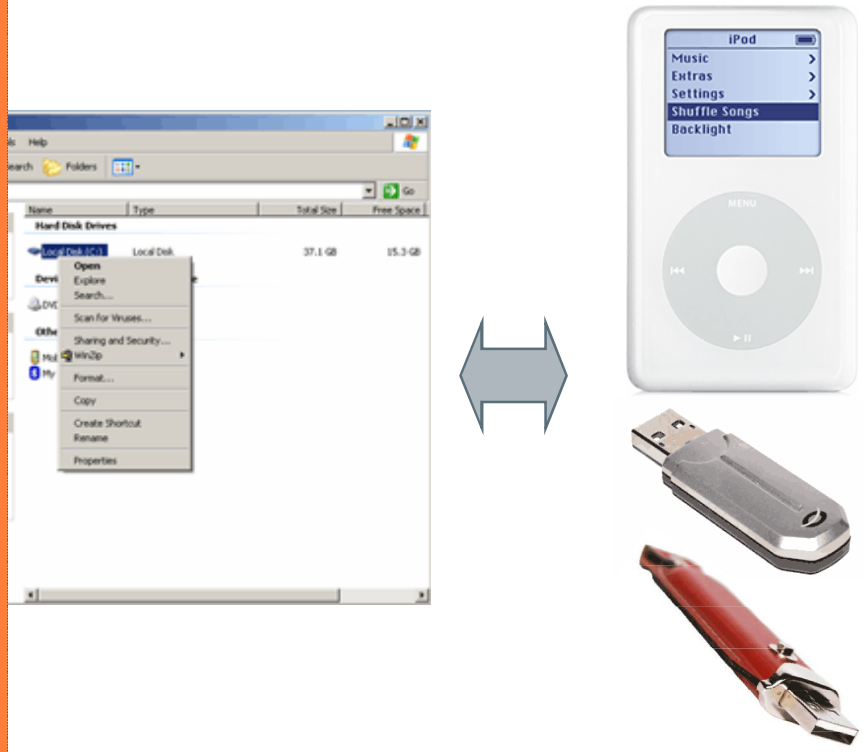
Проблема

Музыкальные файлы?

...или БД Ваших клиентов?

Удобное портативное хранилище?

... или точка входа для вредоносного ПО?



5 минут для копирования 1.500.000 страниц MS Word

Статистика 2010

- **75%** компаний из рейтинга **Fortune 1000** столкнулись с проблемой утечки информации[1]
- Атаки вирусов, неавторизованный доступ, кража/потеря ноутбуков и других мобильных устройств; кражи конфиденциальной информации в **74%** случаях привели к существенным финансовым потерям
- **$5 миллионов** - цена утраченной корпоративной информации (**на 30%** больше чем в прошлом году)
- **в 53%** организаций не знают какая информация была на утерянном USB устройстве
- **7 из 10 (68%) компаний** ежегодно более 6-ти раз сталкиваются с проблемой утечки информации
- **2 из 10 (20%) компаний** сталкиваются с этой проблемой более **22 раз в год**
- **$100 средняя цена 1** случая восстановления утраченной/украденной/потерянной информации[3]
- **42%** IT специалистов считают, меры традиционно принимаемые для защиты конфиденциальной информации бесполезными

Возможности
Lumension Device Control

Почему Lumension Device Control?

- Возможность выяснить масштабы проблемы
  - Device Scanner / Работа в режиме отчетности
- Охват всех известных и неизвестных устройств
  - I/O управление – без блокировки портов
- Низкие затраты ресурсов на конечной точке
  - Драйвер на уровне ядра, высокая производительность
- Драйвер уровня ядра невидим и недоступен
- Простота управления
  - Централизованный менеджмент, интеграция с Active Directory
- Отчетность

Основные возможности – Device Control

- **Централизованный контроль**
- всех устройств ввода/вывода, с использованием принципа «белого списка», при условии, что по умолчанию всё запрещено
  - Съемные USB носители, PDA's, фотоаппараты, камеры, CD/DVD R/W, модемы и др.
- **Политики** использования устройств
  - Интеграция с Active Directory и Novell's eDirectory
  - Политики для отдельных пользователей и групп пользователей
  - Чтение, Чтение/запись, Нет доступа
  - Временный доступ, доступ по расписанию – по дням недели / по часам

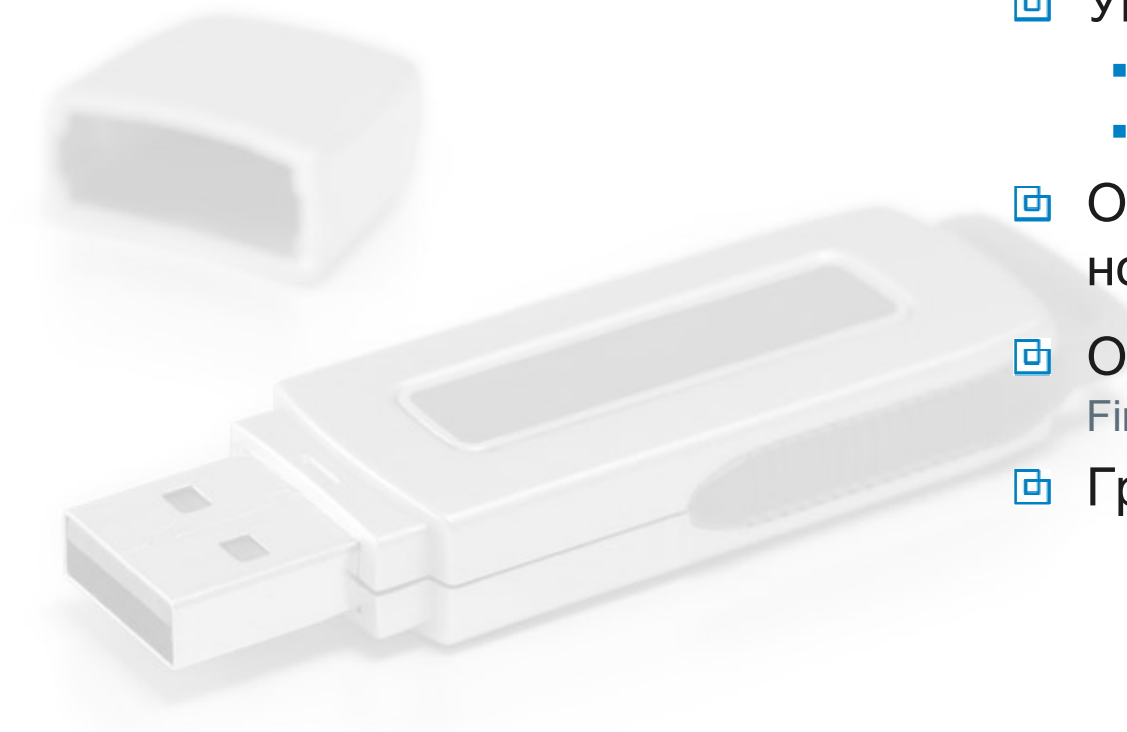
- **Гранулированный контроль**
  - Белые списки по классам устройств и моделям (напр.: разрешаются только Lexar 256MB)
  - Идентификатор уникальных устройств по серийному номеру
  - Авторизация отдельных дисков
  - Определение USB килогеров

Атрибуты доступа

- Read и / или Write
- Доступ по расписанию
  - С 08:00 до 18:00 с понедельника по пятницу
- Временный доступ
  - На следующие 15 минут
  - Начиная со след. понедельника, на 2 дня
- Online / Offline
- Управление квотами
  - Лимит копируемых данных до 100 MB/день

Lumension
IT Secured. Success Optimized.

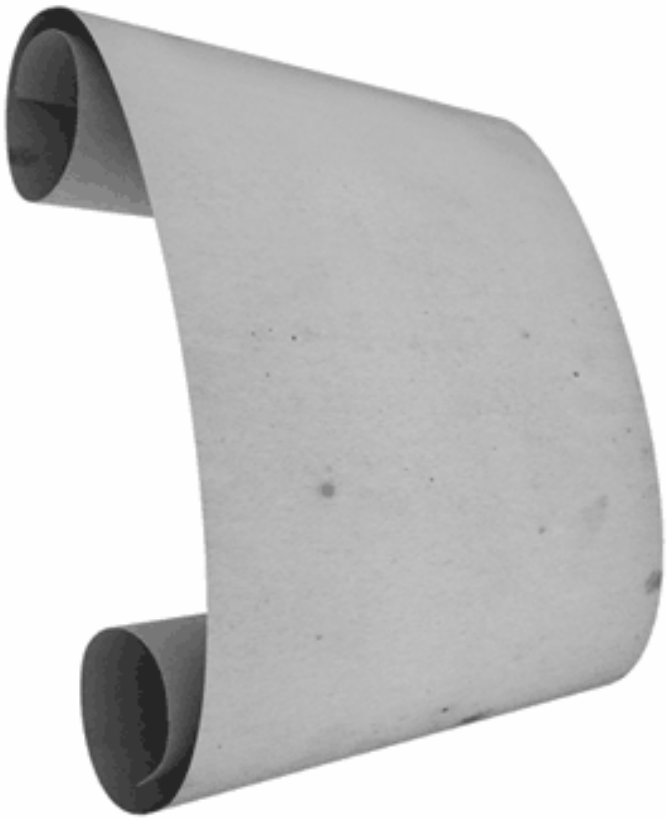
Атрибуты могут быть назначены для...



- Целого класса устройств
  - Все USB принтеры
- Подкласса устройств
  - USB принтер HP 7575, CD/DVD Nec 3520A
- Уникального устройства по
  - шифрованию
  - серийному номеру
- Отдельных CD / DVD носителей
- Отдельной шины (USB, IrDa, Firewire...)
- Групп устройств

Аудит и регистрация

- Регистрация действий пользователя
  - Чтение запрещено / Запись запрещена
  - Устройство подключено / Носитель вставлен
  - *Открытый API для средств отчетности 3-их разработчиков*
- Теневой аудит всех копируемых данных
  - Уровень 1: показывает имена файлов и атрибуты копируемых данных
  - Уровень 2: Перехватывает и сохраняет полные копии данных, записанных ***на*** внешнее устройство или прочитанных ***с*** такого устройства
- Аудит администратора
  - Сохраняет все действия по изменению политик, сделанные администратором SDC



Характеристики безопасности

Драйвер ядра

- Невидим (нет процесса в менеджере задач)
- Быстр (нет потерь производительности)
- Совместим (нет конфликтов с другими приложениями)

Стойкость клиента

- Даже локальный администратор не сможет деинсталлировать клиента

Защита от кейлогеров

Offline защита

- Локальная копия последней версии списка разрешений доступа к устройствам хранится на рабочей станции или ноутбуке, находящемся вне сети

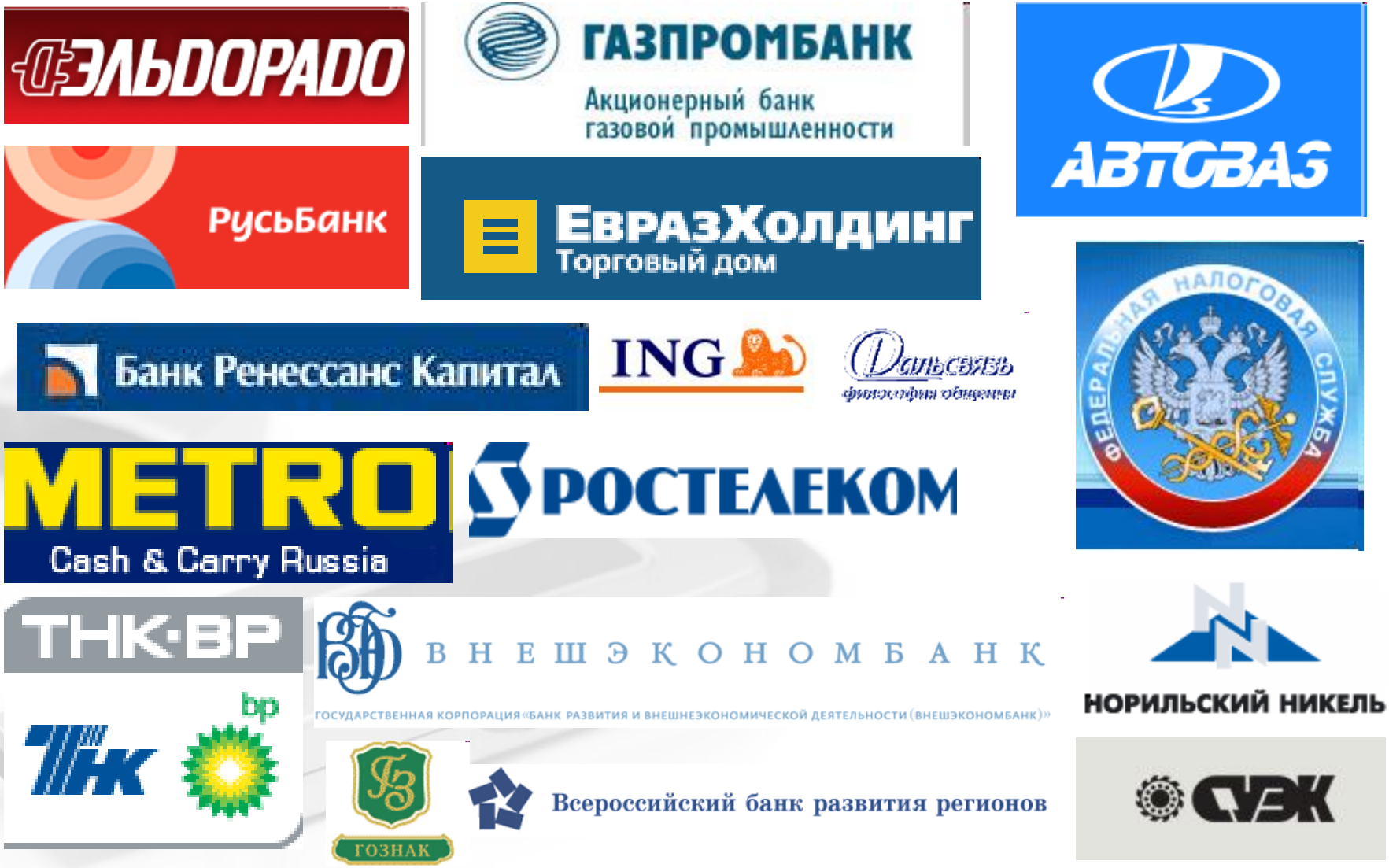
Аудит и логирование

- **Логирование действий пользователя**
  - Чтение запрещено / Запись запрещена
  - Устройство подключено / Носитель вставлен
- **Теневой аудит всех копируемых данных**
  - Уровень 1: показывает имена файлов и атрибуты копируемых данных
  - Уровень 2: Перехватывает и сохраняет полные копии данных, записанных ***на*** внешнее устройство или прочитанных ***с*** такого устройства
- **Аудит администратора**
  - Сохраняет все действия по изменению политик, сделанные администратором LDC

Простота управления

- **Изменение политик offline**
  - Посылает изменения (через файл) на компьютеры, не подключенные к сети
- **Удобное управление политиками**
  - Опция группировки устройств, опция группировки носителей, увеличены возможности аудита, комментарии пользователя к устройствам
- **Многоязыковой интерфейс клиента**
  - Язык интерфейса клиента изменяется на основании региональных установок
- **Применение политик доступа в реальном времени**
- **Режим обучения**
  - Разрешения могут быть присоединены к корню дерева Device Explorer и применены для всех устройств, используемых пользователем(ями) либо группой(ами).
- **Оповещение о событиях (syslog)**
  - Сообщение, подготовленное для пользователя, при отказе в доступе к устройству

Крупнейшие клиенты в РФ



Lumension Endpoint Management and Security Suite

Products

Endpoint Operations

Lumension®
Asset Manager

Lumension®
Power Manager

Lumension®
Content Wizard

Vulnerability Management

Lumension®
Patch and Remediation

Lumension® Scan

Lumension®
Security Configuration Management

Endpoint Protection

Lumension® AntiVirus

Lumension®
Application Control

Lumension®
Endpoint Integrity Service

Data Protection

Lumension®
Device Control

Lumension®
Data Loss Prevention

PGP® Whole Disk Encryption

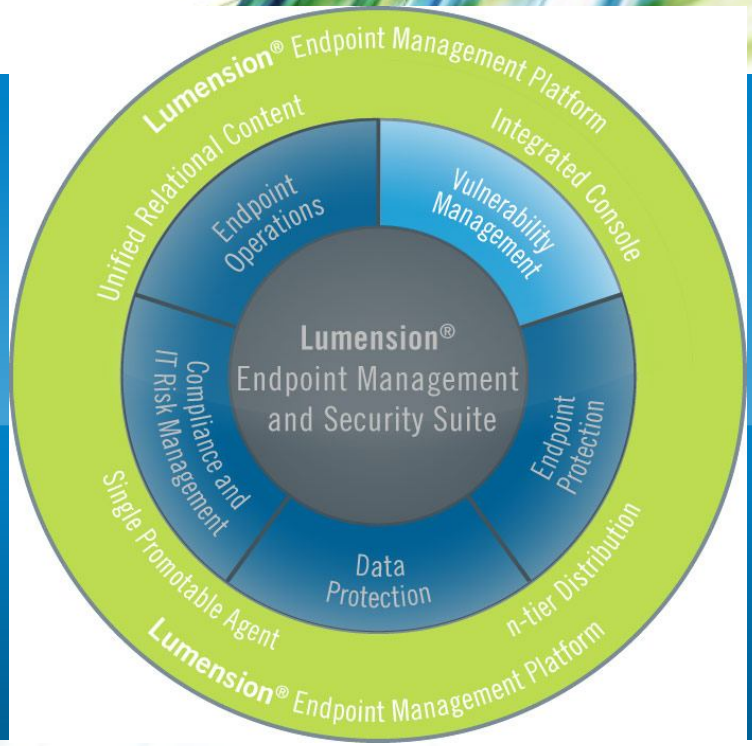
Compliance and IT Risk Management

Lumension®
Risk Manager

Lumension®
Enterprise Reporting

LEMSS: Новая платформа

- **Сокращение TCO – полной стоимости владения**
- **Единая платформа для всех приложений с удобным интуитивным управлением**
- **Быстрый процесс установки и обновления ПО**



Сертификат ФСТЭК

- Федеральная служба технического и экспортного контроля (ФСТЭК) по Системе сертификации средств защиты информации по требованиям безопасности информации (Свидетельство № РОСС RU.0001.01БИ00) приняла решение о проведении сертификации системы защиты информации **«Lumension Device Control»** на соответствие требованиям технических условий ХТРУ.501410.001ТУ.

Спасибо за внимание

headtechnology
it-security

Vulnerability Management I Endpoint Protection I Data Protection I Reporting and Compliance

www.lumension.com

Lumension
IT Secured. Success Optimized.