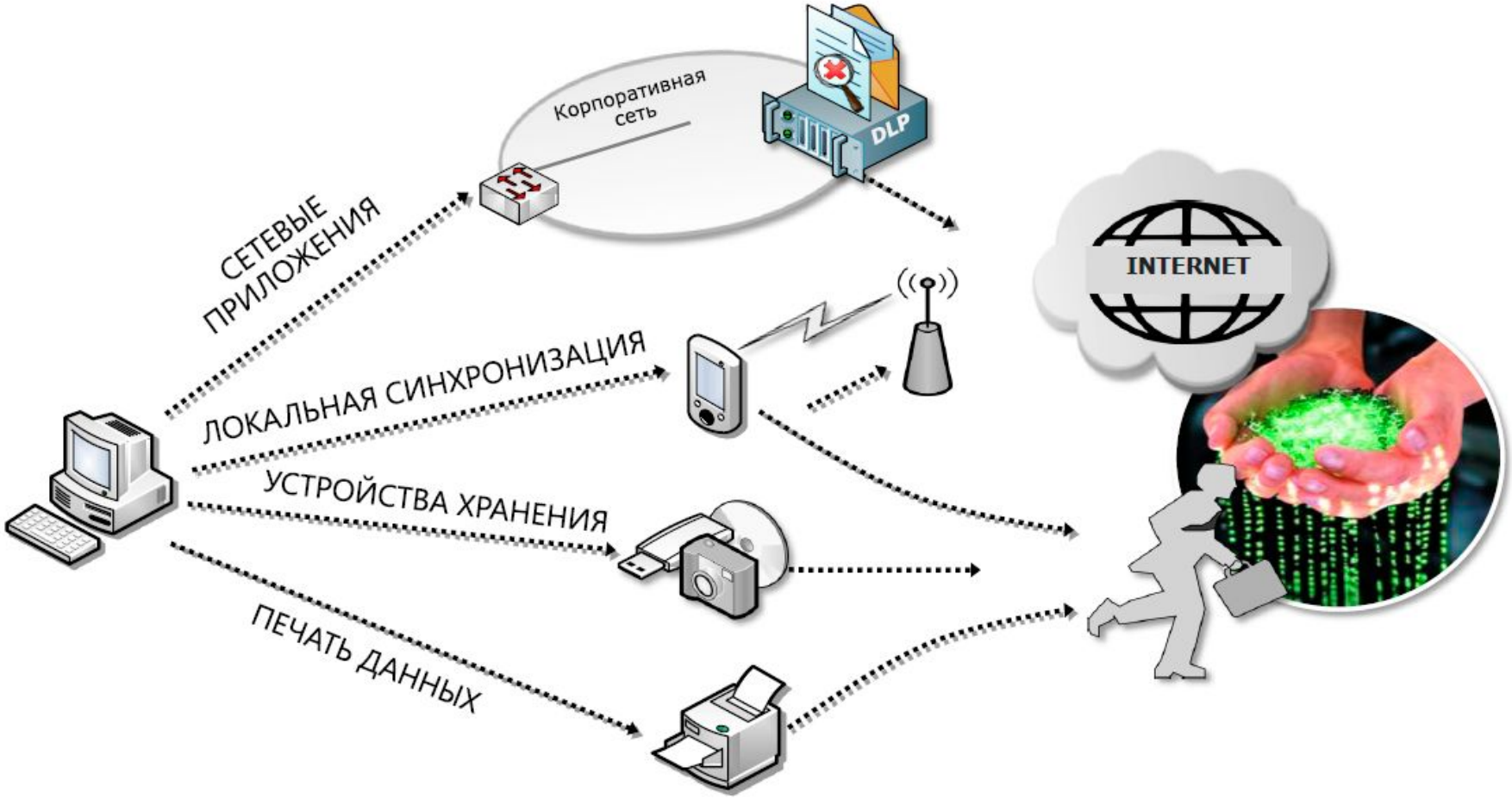
«Механика» утечки данных



Традиционные решения информационной безопасности

ДЛЯ ПОЛНОЦЕННОГО РЕШЕНИЯ ПРОБЛЕМЫ ИНСАЙДЕРСКИХ УТЕЧЕК ДАННЫХ НЕОБХОДИМО ИСПОЛЬЗОВАНИЕ СПЕЦИАЛИЗИРОВАННОГО ПРОДУКТА

ФОКУС НА ВНЕШНИХ УГРОЗАХ

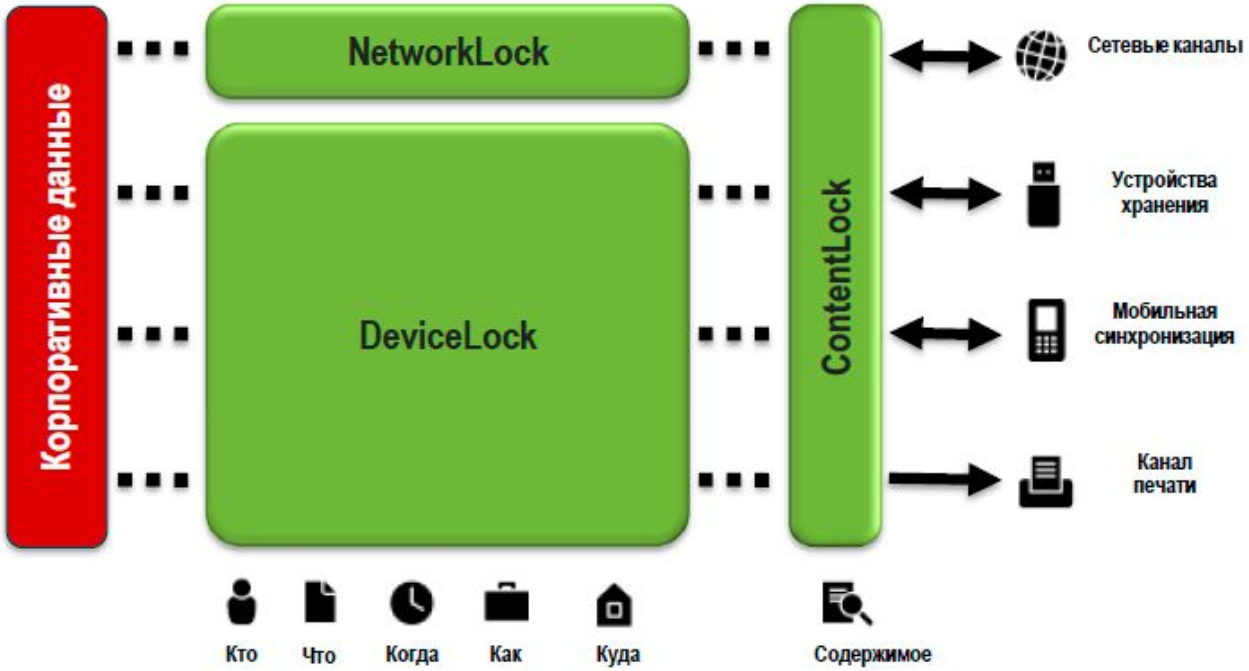
- Защита от хакеров и внешних вторжений (межсетевые экраны, ips)
- Антивирусы, анти-спам, контентные фильтры почты, др.
- Системы авторизации, токены, vpn для доступа пользователей к важной информации извне
- Контролируемые почтовые серверы, средства фильтрации контента

НЕТ КОНТРОЛЯ ЛОКАЛЬНЫХ КАНАЛОВ

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

DeviceLock Endpoint DLP Suite

- Полноценное DLP-решение для защиты от локальных утечек данных
- Модульная архитектура комплекса с независимыми компонентами и опциональным лицензированием
- Применимо для организаций любого типа и размера
- Возможность постепенного и экономного расширение функционала DLP-решения организации в соответствии с реальными потребностями



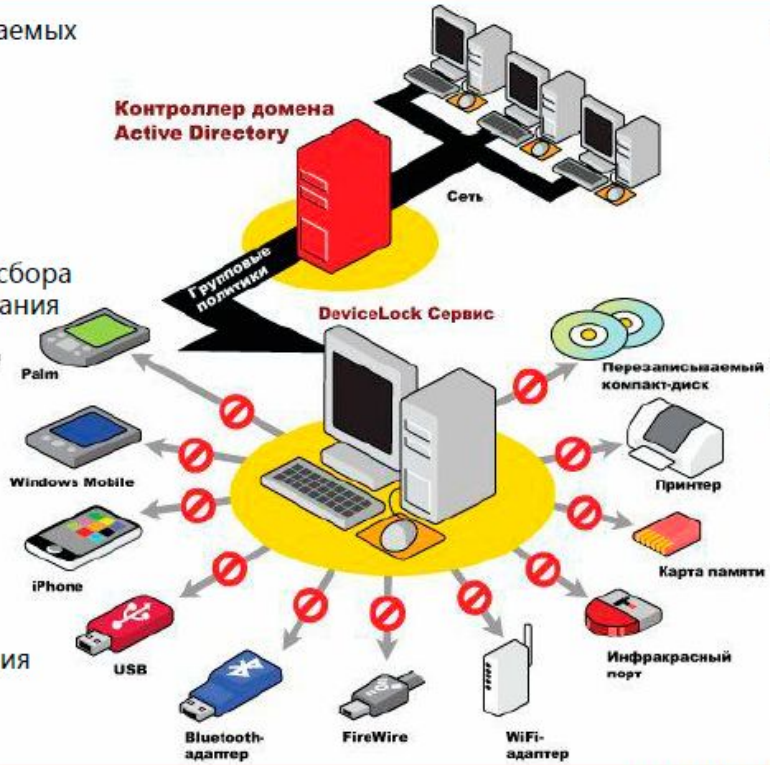
DeviceLock

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



- 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

- Полноценная интеграция управления жизненным циклом агентов в платформу microsoft Active Directory

ГРАНУЛИРОВАННОСТЬ КОНТРОЛЯ

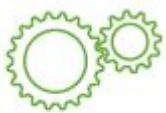
УНИКАЛЬНЫЕ МАСШТАБИРУЕМОСТЬ, ЭКОНОМИЧНОСТЬ И НАДЁЖНОСТЬ

Фундаментальные возможности DeviceLock

- Гранулированный контроль доступа пользователей ко всем типам устройств и портов локальных компьютеров, и в частности канала локальной синхронизации с мобильными устройствами.
- Детальное событийное протоколирование действий пользователей, административных процессов и состояния комплекса, включая теневое копирование данных, с хранением данных в централизованной базе данных и поддержкой собственного сервера полнотекстного поиска данных.
- Интеграция с внешними программными и аппаратными средствами шифрования съемных носителей (определение прав доступа к шифрованным носителям)
- Блокировка аппаратных кейлоггеров (USB и PS/2)
- Задание разных политик для компьютеров в режимах online/offline
- Встроенная защита агентов от несанкционированных воздействий пользователей и локальных администраторов, автоматизированный мониторинг состояния агентов и политик

Основные компоненты DeviceLock

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

DEVICELOCK GROUP POLICY MANAGER

Используется для управления настройками DeviceLock через групповые политики контроллера домена Active Directory.

Компонент NetworkLock - Контроль сетевых протоколов (1/2)

Опциональный компонент, позволяющий осуществлять контроль, аудит и теневое копирование файлов, передаваемых по сети с использованием ряда сетевых протоколов

КОНТРОЛЬ, АУДИТ И ТЕНЕВОЕ КОПИРОВАНИЕ ДЛЯ КАНАЛОВ СЕТЕВЫХ КОММУНИКАЦИЙ.

Детектирование и фильтрация обращений к сетевым приложениям и протоколам, независимо от используемых портов

- Реконструкция сообщений и сессий, с извлечением файлов, данных и параметров
- Аудит и теневое копирование передаваемых файлов и данных
- Теневое копирование файлов и данных, получаемых по протоколам FTP, HTTP, службам мгновенных сообщений

БЕЛЫЙ СПИСОК ДЛЯ РАЗЛИЧНЫХ СЕТЕВЫХ ПРОТОКОЛОВ И IP-АДРЕСОВ

- Расширенный гибкий контроль сетевых протоколов в зависимости от ряда параметров:
  - Диапазоны ip-адресов,
  - Диапазоны портов

Компонент NetworkLock - Контроль сетевых протоколов (2/2)

КОНТРОЛЬ, АУДИТ И ТЕНЕВОЕ КОПИРОВАНИЕ ДЛЯ КАНАЛОВ СЕТЕВЫХ КОММУНИКАЦИЙ:

- Передача почтовых сообщений по обычным и SSL-защищенным SMTP-каналам
  - Раздельный контроль сообщений и сессий
- Веб-доступ по протоколам HTTP/HTTPS, популярные почтовые сервисы и социальные сети
  - веб-почта Gmail™, Yahoo! Mail™, Windows Live® Mail
  - социальные сети Twitter™, Facebook®, LiveJournal™, LinkedIn®, MySpace™, Одноклассники™, ВКонтакте™
- Службы мгновенных сообщений ICQ/AOL, MSN Messenger, Jabber, IRC, Yahoo Messenger, Mail.ru Agent
- Передача файлов по протоколам FTP и FTP-SSL
- Telnet-сессии

Связка с дополнительным компонентом ContentLock для повышения возможностей контроля данных в каналах сетевых коммуникаций

Компонент ContentLock – Контентная фильтрация

- КОНТЕНТНЫЙ АНАЛИЗ И ФИЛЬТРАЦИЯ данных при их копировании через ряд каналов передачи –как локальные (съемные носители данных и устройства хранения данных –CD/DVD, Floppy, Removable), так и сетевые приложения и сервисы (e-mail и web-почта, FTP, службы мгновенных сообщений и социальные сети)
  - Поддержка более 80 форматов файлов и данных
  - Контроль доступа по шаблонам регулярных выражений (RegExp) с различными численными и логическими условиями соответствия шаблона критериям и ключевым словам
  - Встроенные шаблоны для наиболее часто контролируемых данных
    - Номера кредитных карт, банковских счетов, адреса и т.д.
    - Промышленные справочники (Медицинские термины, термины программирования, др.)
- ИЗБИРАТЕЛЬНЫЕ ПОЛИТИКИ ТЕНЕВОГО КОПИРОВАНИЯ (ФИЛЬТРАЦИЯ) файлов и данных, построенные на анализе текстового содержимого и ключевых словах
  - снижение объема данных, хранимых в базе данных теневого копирования, и нагрузки на локальную сеть, вызванную передачей этих данных на сервер с БД теневого копирования

Сервер полнотекстового поиска DeviceLock Search Server

DEVICELOCK SEARCH SERVER (ПОИСКОВЫЙ СЕРВЕР, DLSS)

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